Honeywell

XYR 400E Wireless Ethernet

User's Manual

34-XY-25-26
Version 1
5/1/08

Notices and Trademarks

Copyright 2008 by Honeywell International Inc.
Version 1 May 1, 2008

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customers.

In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell, PlantScape, Experion PKS, and **TotalPlant** are registered trademarks of Honeywell International Inc.

Other brand or product names are trademarks of their respective owners.

Honeywell International

Process Solutions

2500 West Union Hills

Phoenix, AZ 85027

1-800 343-0228

About This Document

This document describes preparation, operation and maintenance of the XYR 400E Ethernet Modem. Mounting, installation and wiring are covered in other documents.

Honeywell does not recommend using devices for critical control where there is a single point of failure or where single points of failure result in unsafe conditions. XYR3000 is targeted at open loop control, supervisory control, and controls that do not have environmental or safety consequences. As with any process control solution, the end-user must weigh the risks and benefits to determine if the products used are the right match for the application based on security, safety, and performance. Additionally, it is up to the end-user to ensure that the control strategy sheds to a safe operating condition if any crucial segment of the control solution fails.

Revision Information

Document Name	Document ID	Version Number	Publication Date
XYR 400E Wireless Ethernet User's Manual	34-XY-25-26		5/1/2008

References

The following list identifies all documents that may be sources of reference for material discussed in this publication.

Document Title
Getting Started with Honeywell One Wireless solutions
XYR3000 MSG
How to build an XYR3000 system

Support and Contact Information

United States and Canada

Contact: Honeywell Solution Support Center
Phone: 1-800 822-7673. In Arizona: 602- 313-5558
Calls are answered by dispatcher between 6:00 am and 4:00 pm Mountain Standard Time. Emergency calls outside normal working hours are received by an answering service and returned within one hour.
Facsimile: (602) 313-3293
Mail: Honeywell TAC, MS P13
2500 West Union Hills Drive
Phoenix, AZ, 85027

World Wide Web

Honeywell Solution Support Online:
http://www.honeywell.com/ps

Elsewhere

Call your nearest Honeywell office.

Training Classes

Honeywell Automation College:

http://www.automationcollege.com

Symbol Definitions

The following table lists those symbols used in this document to denote certain conditions.

Symbol	Definition
	ATTENTION: Identifies information that requires special consideration.
	TIP: Identifies advice or hints for the user, often in terms of performing a task.
CAUTION	Indicates a situation which, if not avoided, may result in equipment or work (data) on the system being damaged or lost, or may result in the inability to properly operate the process.
	CAUTION: Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices. **CAUTION** symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.
	WARNING: Indicates a potentially hazardous situation, which, if not avoided, could result in serious injury or death. **WARNING** symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.
	WARNING, Risk of electrical shock: Potential shock hazard where HAZARDOUS LIVE voltages greater than 30 Vrms, 42.4 Vpeak, or 60 VDC may be accessible.
	ESD HAZARD: Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices.
	Protective Earth (PE) terminal: Provided for connection of the protective earth (green or green/yellow) supply system conductor.
	Functional earth terminal: Used for non-safety purposes such as noise immunity improvement. NOTE: This connection shall be bonded to Protective Earth at the source of supply in accordance with national local electrical code requirements.
	Earth Ground: **Functional earth connection.** NOTE: This connection shall be bonded to Protective Earth at the source of supply in accordance with national and local electrical code requirements.
	Chassis Ground: Identifies a connection to the chassis or frame of the equipment shall be bonded to Protective Earth at the source of supply in accordance with national and local electrical code requirements.

CONTENTS

CHAPTER ONE INTRODUCTION 8

1.1 NETWORK TOPOLOGY 8

1.2 GETTING STARTED QUICKLY 11

CHAPTER TWO INSTALLATION 11

2.1 GENERAL 11

2.2 ANTENNA INSTALLATION 12

2.2.1 Dipole and Collinear antennas 14

2.2.2 Directional antennas. 15

2.3 POWER SUPPLY 16

2.4 SERIAL CONNECTIONS 16

2.4.1 RS232 Serial Port 16

2.4.2 RS485 Serial Port 17

2.5 DISCRETE (DIGITAL) INPUT/OUTPUT 19

CHAPTER THREE OPERATION 19

3.1 START-UP 19

3.2 SELECTING A CHANNEL 21

3.3 DEFAULT CONFIGURATION 23

3.4 CONFIGURING THE UNIT FOR THE FIRST TIME 23

3.4.1 Set PC to same network as XYR 400E 23

3.4.2 Set XYR 400E to same network as PC 26

3.5 NETWORK CONFIGURATION 28

3.6 ETHERNET DATA 30

3.7 NORMAL OPERATION 31

3.8 RADIO CONFIGURATION 32

3.9 SPANNING TREE ALGORITHM / REDUNDANCY 34

3.10 MULTIPLE AP REPEATER MESH NETWORK 35

3.11 ROUTING RULES 42

3.12 WIRELESS MESSAGE FILTERING 45

3.13 SERIAL PORT CONFIGURATION 47

3.13.1 RS-232 PPP Server 47

3.13.2 Serial Gateway 52

3.13.3 Modbus TCP to RTU Gateway 54

3.14 DIGITAL INPUT/OUTPUT 55

3.15 MODBUS I/O TRANSFER 55

3.16 MODULE INFORMATION CONFIGURATION 60

3.17 REMOTE CONFIGURATION 60

3.18 CONFIGURATION EXAMPLES 61

CHAPTER FOUR DIAGNOSTICS 65
4.1 DIAGNOSTICS CHART 65
4.2 DIAGNOSTIC INFORMATION AVAILABLE 66
4.2.1 Connectivity 66
4.2.2 Monitor Communications 67
4.2.3 Statistics 68
4.2.4 Network Traffic Analysis 68
4.3 TESTING RADIO PATHS 68
4.4 UTILITIES 69
4.4.1 PING 69
4.4.2 IPCONFIG 71
4.4.4 ROUTE 72
CHAPTER FIVE SPECIFICATIONS 74
APPENDIX A FIRMWARE UPGRADE 76
APPENDIX B GLOSSARY 82

Chapter One INTRODUCTION

The XYR 400E Industrial WiFi Wireless Ethernet module provides wireless connections between Ethernet devices or Ethernet wired networks (LAN's). It complies with the IEEE 802.11b standard. The XYR 400E has an internal 2.4GHz direct sequence spread spectrum (DSSS) wireless transceiver, which can be used without a radio license in most countries. Users can select one of 11 x 5 MHz wide channels, with the first channel centred at 2.412 GHz.

> *Note that regulations in North America and part of Europe permit all 11 channels to be used in these countries. Please check with your HONEYWELL representative for the permitted channel usage in your country.*

The XYR 400E unit also provides two serial connections as well as the Ethernet connections. It is possible to use all three data connections concurrently, allowing the XYR 400E to act as a ***Device Server.*** Wireless connections can be made between serial devices and Ethernet devices, however appropriate driver applications are required in the host devices to handle the different data format. The XYR 400E does provide connection functionality between serial "Modbus RTU" devices and Ethernet "Modbus TCP" devices.

The XYR 400E is available in two models with different RF power:

XYR 400E-100 100mW of RF power

XYR 400E-300 300mW of RF power

> *Note that European regulations do not permit more than 100mW of RF power to be used. In USA, Canada and Australia, up to 1W of RF power may be generated. In other countries, please check with your HONEYWELL representative.*

The XYR 400E has a standard RJ45 Ethernet connection which will operate at up to 100Mbit/sec. The module will transmit the Ethernet messages on the wireless band at rates between 1 and 11 Mbit/sec.

1.1 Network Topology

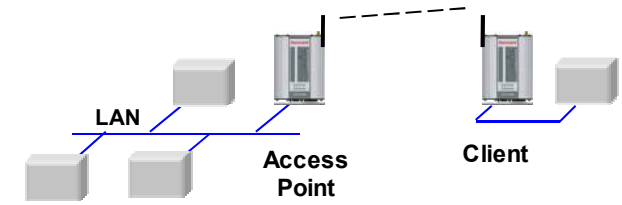
The XYR 400E is an Ethernet device, and must be configured as part of an Ethernet network. Each XYR 400E must be configured as:

- an "Access Point" or a "Client", and
- a "Bridge" or a "Router".

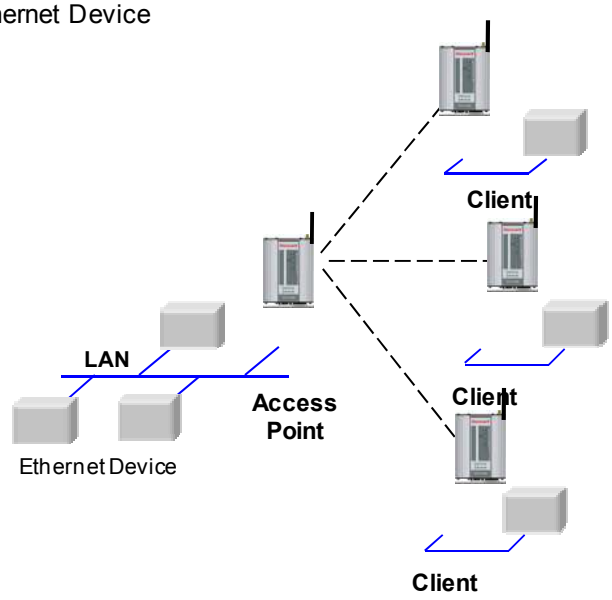
You can also connect to the XYR 400E via a RS232 or RS485 serial port using serial server or PPP (point-to-point) protocol. PPP allows the XYR 400E to connect serial communications into the Ethernet network.

Access Point vs Client

The Access Point unit acts as the "wireless master" unit. The Access Point sets up the wireless links to the Client units, and controls the wireless communications. The first diagram shows two Ethernet devices being linked. One XYR 400E is configured as an Access Point and one as a Client - in this example it doesn't mater which unit is the Access Point.

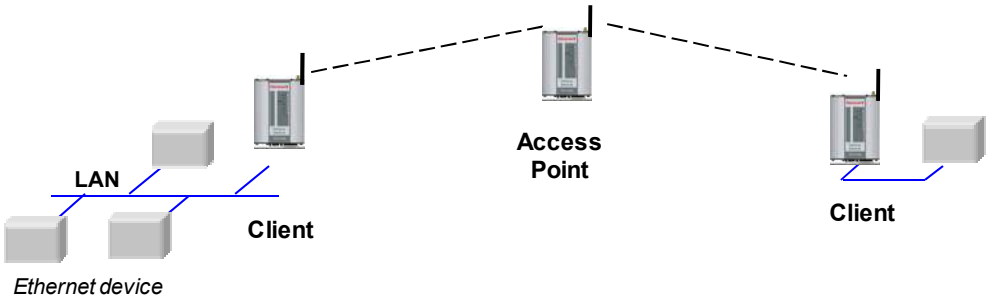


The second diagram shows an existing LAN being extended using XYR 400E's. In this example, the Access Point should be configured at the LAN end - although the wireless link will still work if the Client is at the LAN end.

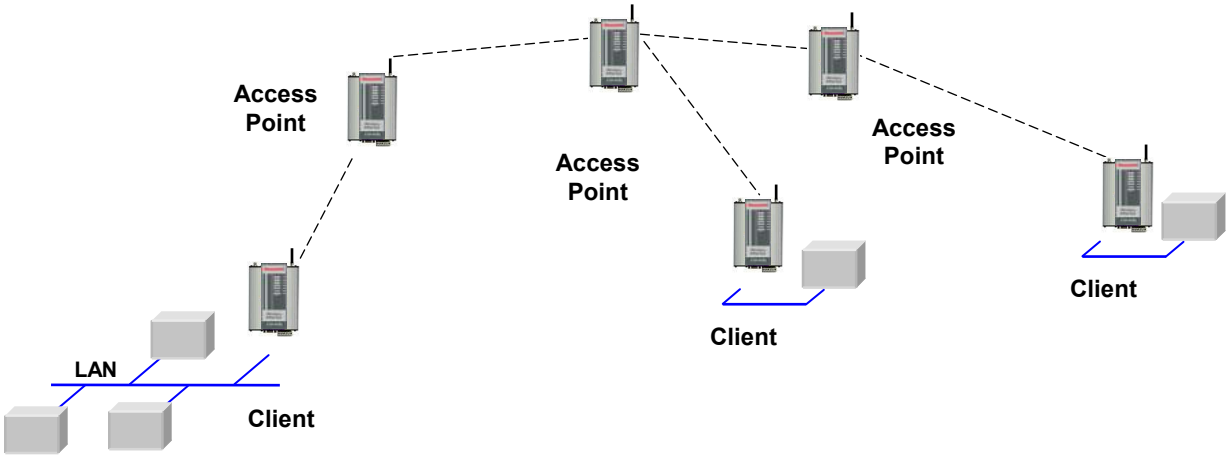


An Access Point can connect to multiple Clients. In this case, the Access Point should be the "central" unit.

An Access Point could be used as a "Repeater" unit to connect two XYR 400E Clients which do not have direct reliable radio paths.



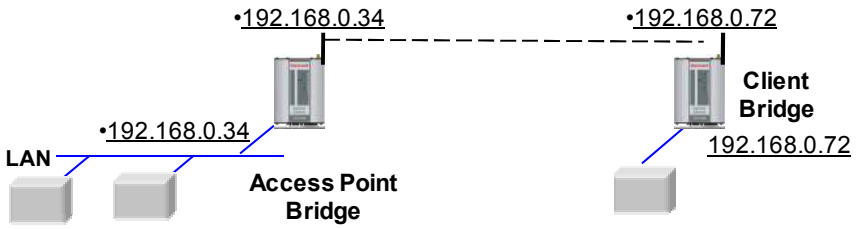
Multiple Access Points can be set-up in a "mesh" network to provide multiple repeaters.



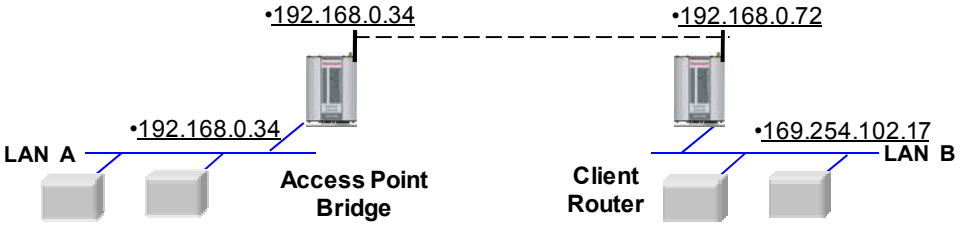
Bridge vs Router

Each XYR 400E is configured with an IP address for the Ethernet side, and another for the wireless side.

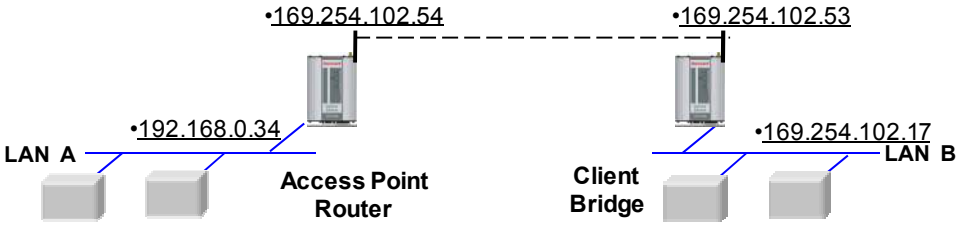
A **Bridge** connects devices within the same Ethernet network - for example, extending an existing Ethernet LAN. For a Bridge, the IP address for the wireless side is the same as the Ethernet side.



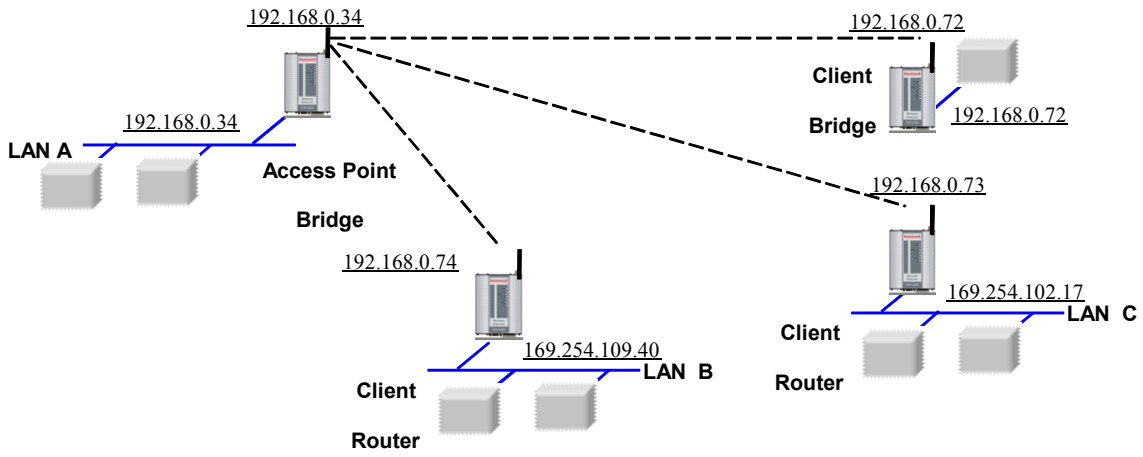
A **Router** connects devices on different LAN's. The IP addresses for the Ethernet and wireless sides are different.



In the above example, the wireless link is part of LAN A, with the Client unit acting as a Router between LAN A and LAN B. Alternately, the Access Point could be configured as a Router - the wireless link is then part of LAN B.



If more than two routers are required within the same radio network, then routing rules may need to be configured (refer section "3.11 Routing Rules" for further details). There is no limit to the number of Bridges in the same network - although there is a limit of 128 Client units linked to any one Access Point.



1.2 Getting Started Quickly

Most applications for the XYR 400E require little configuration. The XYR 400E has many sophisticated features, however if you don't require these features, this section will allow you to configure the units quickly.

First, read Section 2, "Installation". The XYR 400E requires an antenna and a power supply.

- Power the XYR 400E and make an Ethernet connection to your PC (for further information on how to do this, refer to section 3.4)
- Set the XYR 400E address settings as per section 3.4
- Save the configuration - the XYR 400E is now ready to use.

Before installing the XYR 400E, bench test the system. It is a lot easier to locate problems when the equipment is all together.

There are other configuration settings which may or may not improve the operation of the system. For details on these settings, refer to section 3.

Chapter Two INSTALLATION

2.1 General

The XYR 400E module is housed in an rugged aluminium case, suitable for DIN-rail mounting. Terminals will accept wires up to 2.5 sqmm (12 gauge) in size.

All connections to the module must be SELV. Normal 110-250V mains supply should not be connected to any terminal of the XYR 400E module. Refer to Section 2.3 **Power Supply**.

Before installing a new system, it is preferable to bench test the complete system. Configuration problems are easier to recognize when the system units are adjacent. Following installation, the most common problem is poor communications caused by incorrectly installed antennas, or radio

interference on the same channel, or the radio path being inadequate. If the radio path is a problem (i.e. path too long, or obstructions in the way), then higher performance antennas or a higher mounting point for the antenna may rectify the problem. Alternately, use an intermediate XYR 400E Module as a repeater.

The foldout sheet XYR 400E ***Installation Guide*** provides an installation drawing appropriate to most applications. Further information is detailed below.

Each XYR 400E module should be effectively earthed via the "GND" terminal on the XYR 400E module - this is to ensure that the surge protection circuits inside the XYR 400E module are effective.

2.2 Antenna Installation

The XYR 400E module will operate reliably over large distances. The distance which may be reliably achieved will vary with each application - depending on the type and location of antennas, the degree of radio interference, and obstructions (such as buildings or trees) to the radio path.

The maximum range achievable depends on the regulated RF power permitted in your country, and whether you use separate transmit and receive antennas. With a single antenna, 5 km (3 miles) can be achieved in USA, Canada and Australia (4W ERP) and 1km in Europe (100mW ERP). With separate transmit and receive antennas, more than 10km (6 miles) can be achieved in USA, Canada and Australia and more than 5 km in Europe.

To achieve the maximum transmission distance, the antennas should be raised above intermediate obstructions so the radio path is true “line of sight”. The modules will operate reliably with some obstruction of the radio path, although the reliable distance will be reduced. Obstructions which are close to either antenna will have more of a blocking affect than obstructions in the middle of the radio path. The XYR 400E modules provide a diagnostic feature which displays the radio signal strength of transmissions (refer *Diagnostics* section).

Line-of-sight paths are only necessary to obtain the maximum range. Obstructions will reduce the range, however may not prevent a reliable path. A larger amount of obstruction can be tolerated for shorter distances. For short distances, it is possible to mount the antennas inside buildings. An obstructed path requires testing to determine if the path will be reliable - refer the section 6 of this manual.

Where it is not possible to achieve reliable communications between two XYR 400E modules, then a third XYR 400E module may be used to receive the message and re-transmit it. This module is referred to as a repeater. This module may also have a host device connected to it.

The XYR 400E unit has two antenna connections at the top of the module, allowing two antennas to be fitted to the unit. The left connector (looking at the front) labeled “RX” is connected only to the internal wireless receiver. The right connector labeled TX/RX is connected to both the transmitter and receiver.

Note: when only one antenna is used, it must be connected to the right TX/RX connector.

Plant and factory installations

Most installations in industrial plants and factories use a single omni-directional antennas. Installations can suffer from "multi-path fading" effects where multiple reflected radio signals adversely affect the signal strength. This can be checked by moving the antenna a short distance (10 cm or 4 inches) - if the signal increases significantly then there are multi-path effects.

In a "static" installation, where the radio path is not changing, moving an antenna to the position of maximum signal solves this problem. However where the radio path changes because the XYR 400E is mounted on moving equipment, or if there is moving equipment in the area, then the solution is to use two antennas. Because the two connectors are separated, the RF signal at each connector will be different in the presence of multi-path fading. The XYR 400E unit will automatically select the higher RF signal.

Note that directional antennas are not normally used in plant and factory installations.

Line-of-sight installations

In longer line-of-sight installations, the range may be increased by using a high gain antenna on the TX/RX connector. However the gain should not cause the effective radiated power (ERP) to exceed the permitted value. A second higher gain antenna can be connected to the RX connector without affecting ERP - this will increase the operating range provided the background noise in the area is low.

Antennas

Antennas can be either connected directly to the module connectors or connected via 50 ohm coaxial cable (eg RG58 Cellfoil or RG213) terminated with a male SMA coaxial connector. The higher the antenna is mounted, the greater the transmission range will be, however as the length of coaxial cable increases so do cable losses.

The net gain of an antenna/cable configuration is the gain of the antenna (in dBi) less the loss in the coaxial cable (in dB). The maximum net gain of the antenna/cable configuration connected to the TX/RX connector is 0dB in Europe (100mW ERP). In USA, Canada and Australia (4W ERP), the maximum gain is 12dB for the XYR 400E-300 or 16dB for the XYR 400E-100. There is no gain restriction for antennas connected to the RX connector.

The gains and losses of typical antennas are

Antenna	*Gain (dBi)*
Dipole	2
Collinear	5 or 8
Directional	10 - 28
Cable type	*Loss (dB per 10 m / 30 ft)*
RG58 Cellfoil	-6
RG213	-5
LDF4-50	-1.5

The net gain of the antenna/cable configuration is determined by adding the antenna gain and the cable loss. For example, a 5dBi antenna with 10 metres of Cellfoil has a net gain of -1 dB (5dB – 6dB).

Installation tips

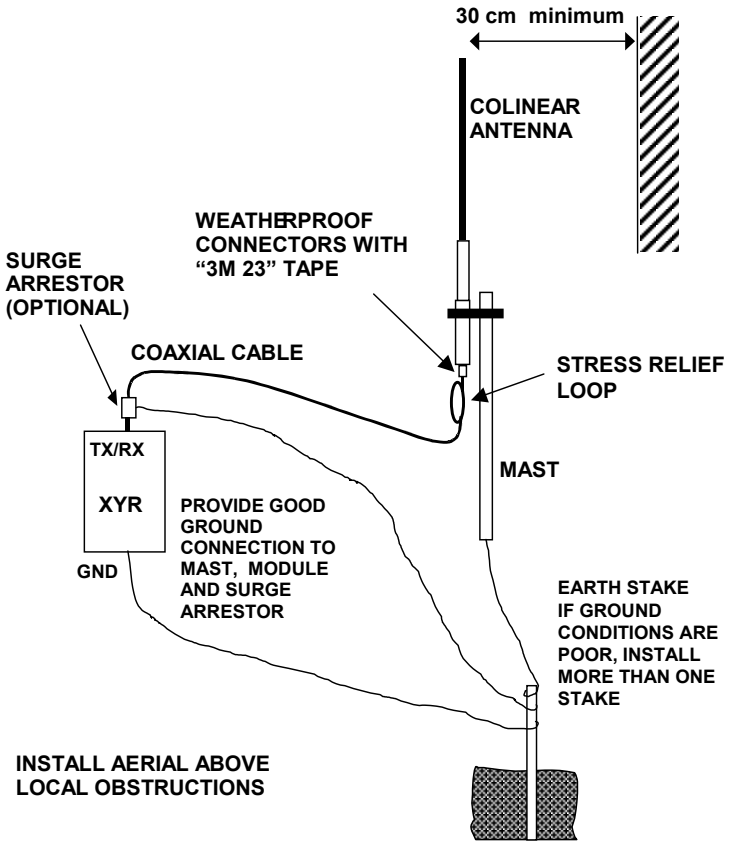
Connections between the antenna and coaxial cable should be carefully taped to prevent ingress of moisture. Moisture ingress in the coaxial cable is a common cause for problems with radio systems, as it greatly increases the radio losses. We recommend that the connection be taped, firstly with a layer of PVC Tape, then with a vulcanizing tape such as "3M 23 tape", and finally with another layer of PVC UV Stabilized insulating tape. The first layer of tape allows the joint to be easily inspected when trouble shooting as the vulcanizing seal can be easily removed.

Where antennas are mounted on elevated masts, the masts should be effectively earthed to avoid lightning surges. For high lightning risk areas, surge suppression devices between the module and the antenna are recommended. If the antenna is not already shielded from lightning strike by an adjacent earthed structure, a lightning rod may be installed above the antenna to provide shielding.

2.2.1 Dipole and Collinear antennas

A dipole or collinear antenna transmits the same amount of radio power in all directions - as such that are easy to install and use. The dipole antenna with integral 5 metres (15 feet) cable does not require any additional coaxial cable, however a cable must be used with the collinear antennas.

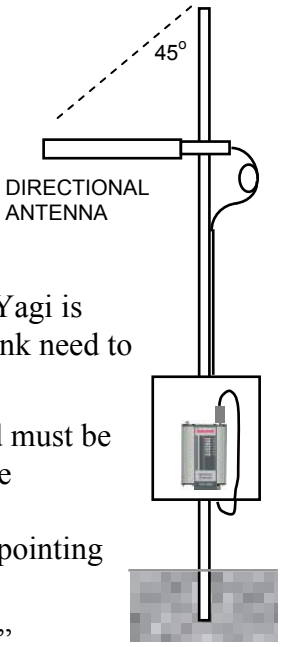
Collinear and dipole antennas should be mounted vertically, preferably 30 cm (1 foot) away from a wall or mast to obtain maximum range.



2.2.2 Directional antennas.

Directional antennas can be

- a Yagi antenna with a main beam and orthogonal elements, or
- a directional radome, which is cylindrical in shape, or
- a parabolic antenna.



A directional antenna provides high gain in the forward direction, but lower gain in other directions. This may be used to compensate for coaxial cable loss for installations with marginal radio path.

Yagi antennas should be installed with the main beam horizontal, pointing in the forward direction. If the Yagi is transmitting to a vertically mounted omni-directional antenna, then the Yagi elements should be vertical. If the Yagi is transmitting to another Yagi, then the elements at each end of the wireless link need to in the same plane (horizontal or vertical).

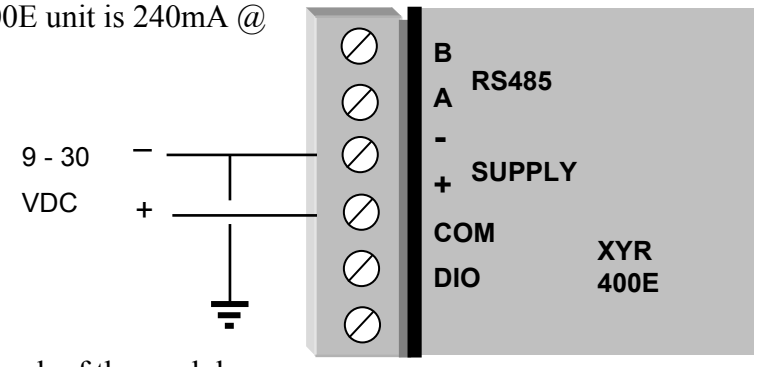
Directional radomes should be installed with the central beam horizontal and must be pointed exactly in the direction of transmission to benefit from the gain of the antenna. Parabolic antennas should be mounted as per the manufacturer's instructions, with the parabolic grid at the "back" and the radiating element pointing in the direction of the transmission.

Ensure that the antenna mounting bracket is well connected to "ground/earth".

2.3 Power Supply

The XYR 400E module can be powered from a 9 - 30VDC power supply. The power supply should be rated at 1 Amp. The positive side of the supply must not be connected to earth. The supply negative is connected to the unit case internally. The DC supply may be a floating supply or negatively grounded.

The power requirements of the XYR 400E unit is 240mA @ 12V or 150mA @ 24VDC. This is inclusive of radio and Ethernet ports active, & serial port plugged in. Transmission current is nominally 350mA at 12V (200mA at 24V) for the 100mW RF unit, and 500mA at 12V (350mA at 24V) for the 300mW RF unit.

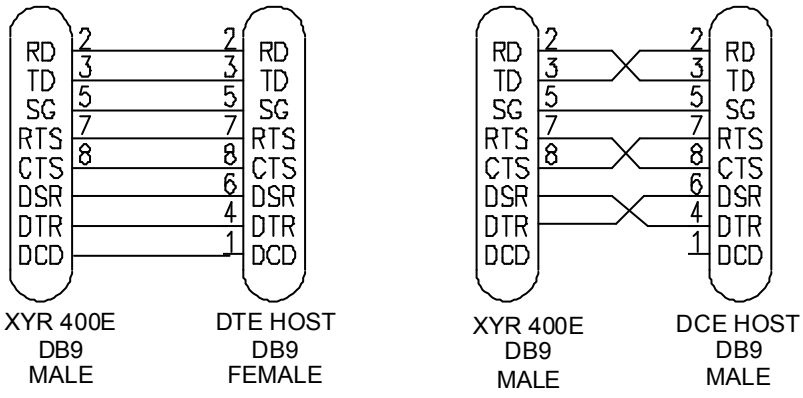


A Ground Terminal is provided on the back of the module. This Terminal should be connected to the Main Ground point of the installation in order to provide efficient surge protection for the module (refer to the Installation Diagram)

2.4 Serial Connections

2.4.1 RS232 Serial Port

The serial port is a 9 pin DB9 female and provides for connection to a host device as well as a PC terminal for configuration, field testing and for factory testing. Communication is via standard RS232 signals. The XYR 400E is configured as DCE equipment with the pinouts detailed below.



Hardware handshaking using the CTS/RTS lines is provided. The CTS/RTS lines may be used to reflect the status of the local unit's input buffer. The XYR 400E does not support XON/XOFF.

Example cable drawings for connection to a DTE host (a PC) or another DCE hosts (or modem) are detailed above.

DB9 Connector Pinouts

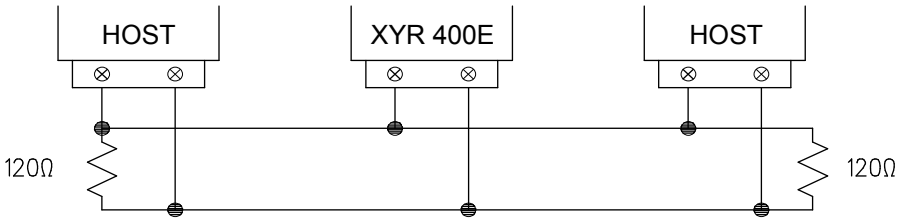
Pin	Name	Direction	Function
1	DCD	Out	**Data carrier detect** –
2	RD	Out	**Transmit Data** – Serial Data Output
3	TD	In	**Receive Data** – Serial Data Input
4	DTR	In	**Data Terminal Ready** -
5	SG		**Signal Ground**
6	DSR	Out	**Data Set Ready** - always high when unit is powered on.
7	RTS	In	**Request to Send -**
8	CTS	Out	**Clear to send -**
9	RI		**Ring indicator** -

2.4.2 RS485 Serial Port

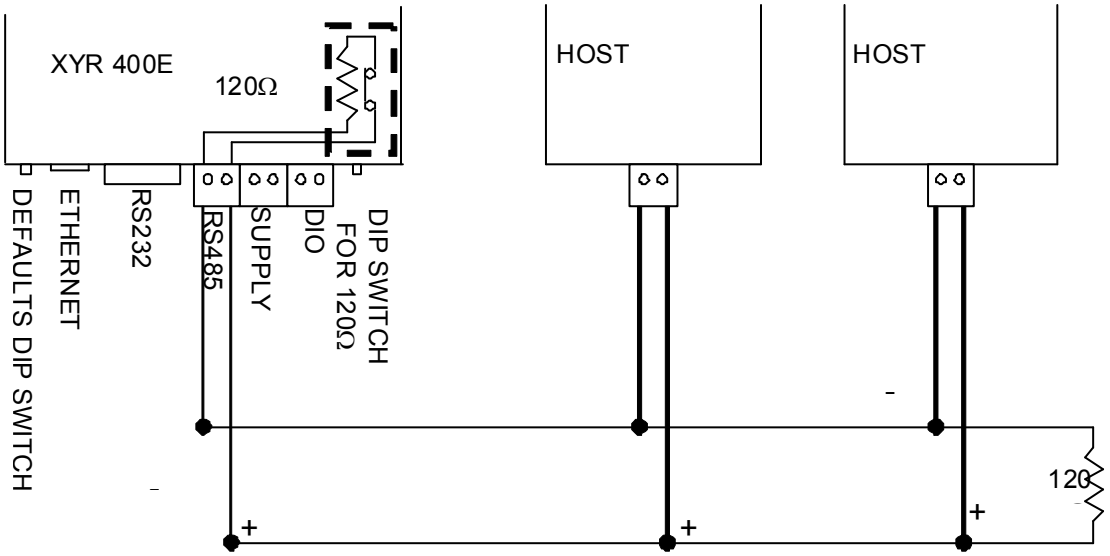
The RS485 port provides for communication between the XYR 400E unit and its host device using a multi-drop cable. Up to 32 devices may be connected in each multi-drop network.

As the RS485 communication medium is shared, only one of the units on the RS485 cable may send data at any one time. Thus communication protocols based on the RS-485 standard require some type of arbitration.

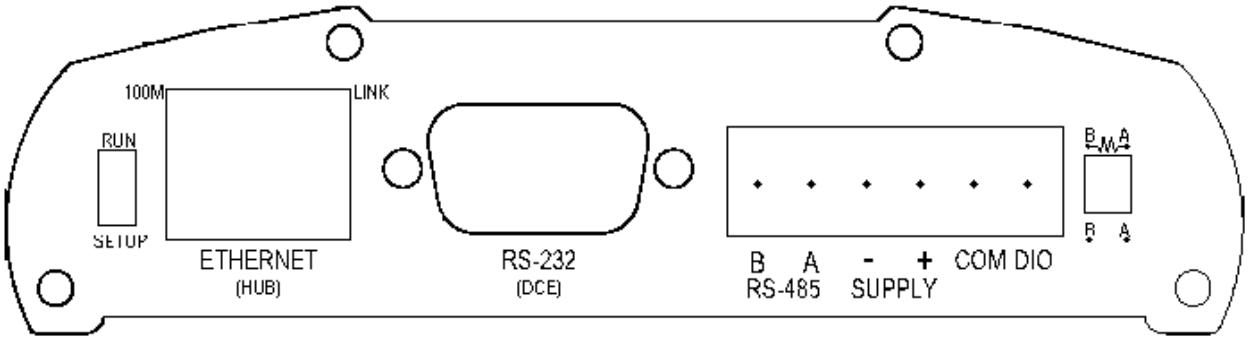
RS485 is a balanced, differential standard but it is recommended that shielded, twisted pair cable be used to interconnect modules to reduce potential RFI. It is important to maintain the polarity of the two RS485 wires. An RS485 network should be wired as indicated in the diagram below and terminated at each end of the network with a 120 ohm resistor. On-board 120 ohm resistors are provided and may be engaged by operating the single DIP switch in the end plate next to the RS485 terminals. The DIP switch should be in the "1" or "on" position to connect the resistor. If the module is not at one end of the RS485 cable, the switch should be off.



RS485 CONNECTIONS



RS485 CONNECTION USING TERMINATING RESISTOR

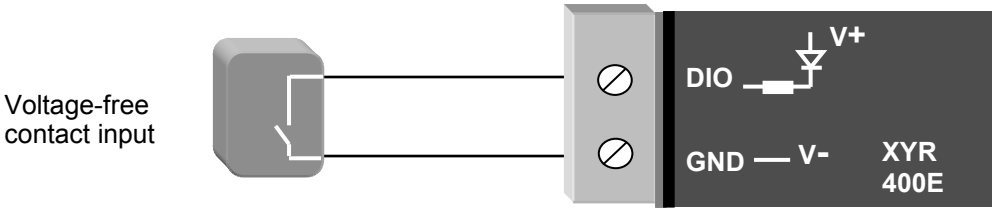


2.5 Discrete (Digital) Input/Output

The XYR 400E has one on-board discrete/digital I/O channel. This channel can act as either a discrete input or discrete output. It can be monitored, or set remotely, or alternatively used to output a communications alarm status.

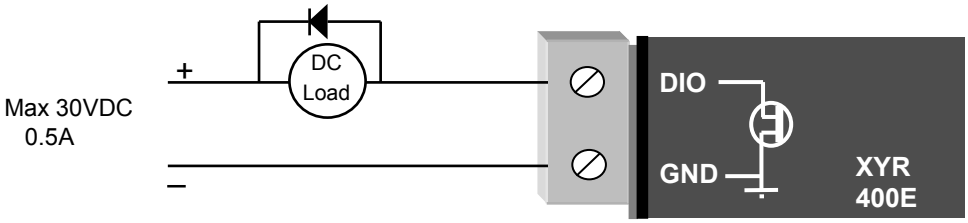
If used as an “input”, the I/O channel is suitable for voltage free contacts (such as mechanical switches) or NPN transistor devices (such as electronic proximity switches). PNP transistor devices are not suitable. Contact wetting current of approximately 5mA is provided to maintain reliable operation of driving relays.

The digital input is connected between the "DIO" terminal and common "COM". The I/O circuit includes a LED indicator which is lit when the digital input is active, that is, when the input circuit is closed. Provided the resistance of the switching device is less than 200 ohms, the device will be able to activate the digital input.



The I/O channel may also be used as a discrete output. The digital outputs are transistor switched DC signals, FET output to common rated at 30VDC 500 mA.

The output circuit is connected to the "DIO" terminal. The digital output circuit includes a LED indicator which is lit when the digital output is active.



Chapter Three OPERATION

3.1 Start-up

“Access Point” Start-up

An Access Point (AP) unit starts and immediately begins transmitting periodic messages, called beacons, on the configured channel. Beacons include capability information that a Client may examine in order to identify if the Access Point is suitable for link establishment. Clients will only

attempt to establish a link with an Access Point whose beacon indicates a matching SSID. Access Points do not initiate link establishment.

"Client" Start-up

When a Client powers up, it scans for beacons from Access Points. While a link is not established, the Client cyclically scans all available channels for a suitable Access Point. The Client will attempt to establish a link with an Access Point only if it has matching SSID and other compatible capabilities as indicated by the beacon. If more than one suitable Access Point is discovered, the client will attempt to establish a link with the Access Point that has the strongest radio signal.

Link Establishment

Once a Client identifies a suitable Access Point for link establishment it attempts to establish a link using a two step process – "Authentication" and "Association". During Authentication the Client and Access Point check if their configurations permit them to establish a link. Once the Client has been authenticated, it will then request an Association to establish a link.

Status of the wireless link is indicated via the Link LED. For an Access Point, the Link LED will be OFF while no links have been established. Once one or more links have been established, the Link LED is ON. For a Client, the Link LED will reflect the connection status to an Access Point. Link status is also displayed on the "Connectivity" page of the web interface.

After the link is established, data may be transferred in both directions. The Access Point will act as a master-unit and will control the flow of data to the Clients linked to it. Clients can only transmit data to the AP to which they are connected. When a Client transfers data to another Client, it first transmits the data to the AP which then forwards the data to the destined Client.

Presence of a "link" does not mean that the connected unit is authorized to communicate over radio. If the encryption keys are incorrect between units in the same system, or a dissimilar encryption scheme is configured, the LINK led will light, however data may not be passed over the wireless network.

A maximum of 255 Clients may be linked to an Access Point.

How a Link connection is lost

The Access Point refreshes the link status with a Client every time a message is received from that Client. If nothing is received from a Client for a period of 120 seconds, the Access Point sends a "link-check" message. If there is no response to the link-check a De-authenticate message is sent and the link is dropped.

A Client monitors beacons from an Access Point to determine whether the link is still present. If the Client can no longer receive beacons from the AP, the AP is considered to be out-of-range and the link is dropped. Whenever a Client is not connected to an AP, it will cyclically scan all available channels for a suitable AP.

Roaming

Clients may also *roam* between Access Points. If a Client receives a beacon from an AP with a stronger signal than the current AP (providing SSID is the same and capability information are compatible), it may disconnect from the first AP and establish a link with the second AP. This functionality permits a client to have mobility whilst maintaining a link with the most suitable AP.

LED Indication

The following table details the status of the indicating LEDs on the front panel under **normal** operating conditions.

LED Indicator	Condition	Meaning
OK	GREEN	Normal Operation
OK	RED	Supply voltage too low.
Radio RX	GREEN flash	Radio receiving data
Radio RX	RED flash	Weak radio signal
Radio TX	Flash	Radio Transmitting
Radio LINK	On	On when a radio communications link is established
Radio LINK	Off	Communications failure or radio link not established
Radio LINK	GREEN flash RED flash	Serial Port Receiving CTS low
LAN	ON	Link Established on Ethernet port
LAN	Flash	Activity on Ethernet port.
Serial	GREEN flash	Rs232 Serial Port Activity
Serial	RED flash	Rs485 Serial Port Activity
DIO	On	Digital Output ON ***or*** Input is grounded.
DIO	Off	Digital Output OFF ***and*** Input is open circuit.

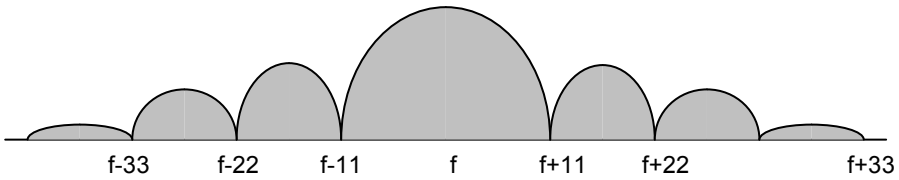
The Ethernet RJ45 port incorporates two indication LEDs. The LINK LED comes on when there is a connection on the Ethernet port, and will blink off briefly when activity is detected on the Ethernet Port. The 100MB LED indicates that the connection is at 100 MBit/Sec. The 100MB LED will be off for 10MB/Sec connection.

Other conditions indicating a fault are described in Chapter Six **Troubleshooting**.

3.2 Selecting a Channel

The XYR 400E conforms to the IEEE 802.11 Wireless LAN specification. The XYR 400E supports 11 radio channels, each 5MHz wide, in the range 2412MHz to 2462MHz. Only one of these channels is used for a connection. The desired channel is selected and configured at the Access Point, and is then used for all beacon transmissions and connections. Clients scan all 11 channels for a suitable Access Point and then adopt the same channel as the AP when a connection

is established. Although each channel is only 5MHz wide, the radio transmission is a lot wider. Hence the channels *overlap*. The following diagram shows the RF energy distribution for a WiFi transmission:



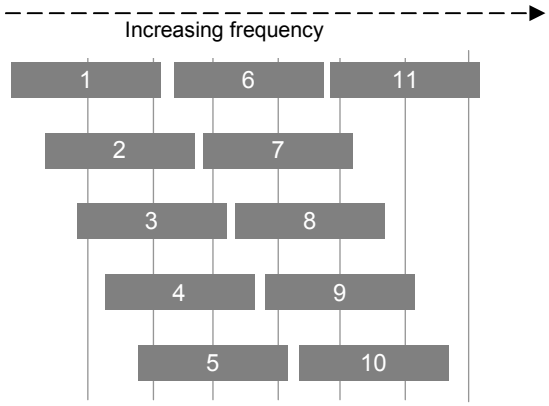
RF power distribution in a WiFi transmission with channel central frequency, f

Most of the energy is in a central 22 MHz wide "lobe", centred around the channel frequency, however there are also side-lobes extending either side.

If we ignore the side lobes and consider each WiFi message as a 22MHz wide transmission, then the following diagram represents how transmissions in each channel overlaps.

If there is more than one WiFi AP within the same wireless range, then it is important that the AP's are on channels as far apart as possible. If there are only two AP's, then set them to 1 and 11. If there are three, set them to 1, 6, 11.

It is also important that correct channel is selected for region. Channels 1 to 11 are approved for North America (FCC), Europe (ETSI), Canada (IC) and Australia (ACMA). Channels 10 and 11 are approved for use in Spain and France. Refer to the relevant regulatory authority for the region as to which radio channels are approved for use.



3.3 Default Configuration

The default factory configuration of the XYR 400E is

- Client/Bridge/
- IP address192.168.0.1XX, where XX is the last two digits of the serial number (the default IP address is shown on the printed label on the back of the module)
- netmask 255.255.255.0
- Username is "*user*" and the default password is "*user*"

The XYR 400E will temporarily load some factory-default settings if powered up with the Factory Default switch (on the end-plate of the module) in SETUP position. When in SETUP mode, wireless operation is disabled. The previous configuration remains stored in non-volatile memory and will only change if a configuration parameter is modified and the change saved.

> ***Do not forget*** *to set the switch back to the RUN position and cycle power at the conclusion of configuration for resumption of normal operation.*

3.4 Configuring the Unit for the First Time

The XYR 400E has a built-in web server, containing webpages for analysis and modification of configuration. The configuration can be accessed using Microsoft® Internet Explorer. This program is shipped with Microsoft Windows or may be obtained freely via the Microsoft® website.

Configuration of IP address, gateway address and subnet mask may also be accessed via the RS-232 serial port.

Accessing Configuration for the first time

There are two methods for accessing the configuration inside a XYR 400E. The first method requires changing your computer settings so that the configuring PC is on the same network as the XYR 400E with factory default settings. **This is the preferred method** and is much less complicated than the second method. You will need a "straight-through" Ethernet cable between the PC Ethernet port and the XYR 400E. The factory default Ethernet address for the XYR 400E is 192.168.0.1XX where XX are the last two digits of the serial number (check the label on the back of the module).

The second method requires setting an IP address in the XYR 400E such that it is accessible on your network without having to change your network settings.

3.4.1 Set PC to same network as XYR 400E

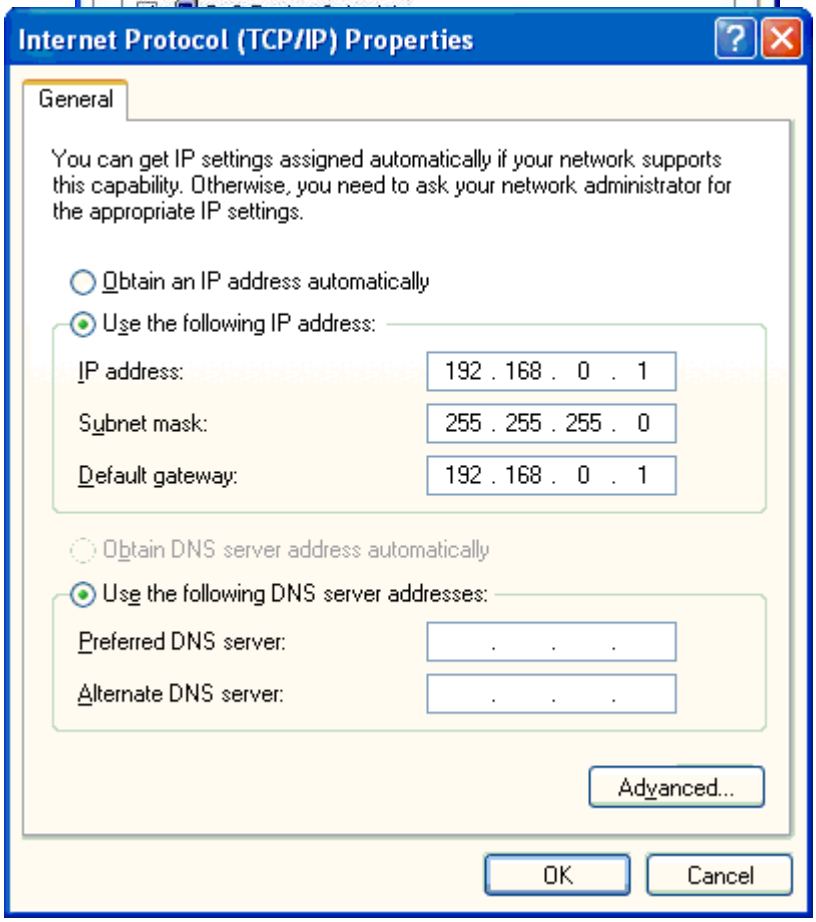
Connect the Ethernet cable between unit and the PC configuring the module.

- Set the Factory Default Switch to the SETUP position. This will always start the XYR 400E with Ethernet IP address 192.168.0.1XX, subnet mask 255.255.255.0, gateway IP 192.168.0.1 and the radio disabled. **Do not forget** to set the switch back to the RUN position and cycle power at the conclusion of configuration for resumption of normal operation.

- Power up the XYR 400E module.
- Open “Network Settings” on your PC under Control Panel. The following description is for Windows XP - earlier Windows operating systems have similar settings.

- Open “Properties” of Local Area Connection.

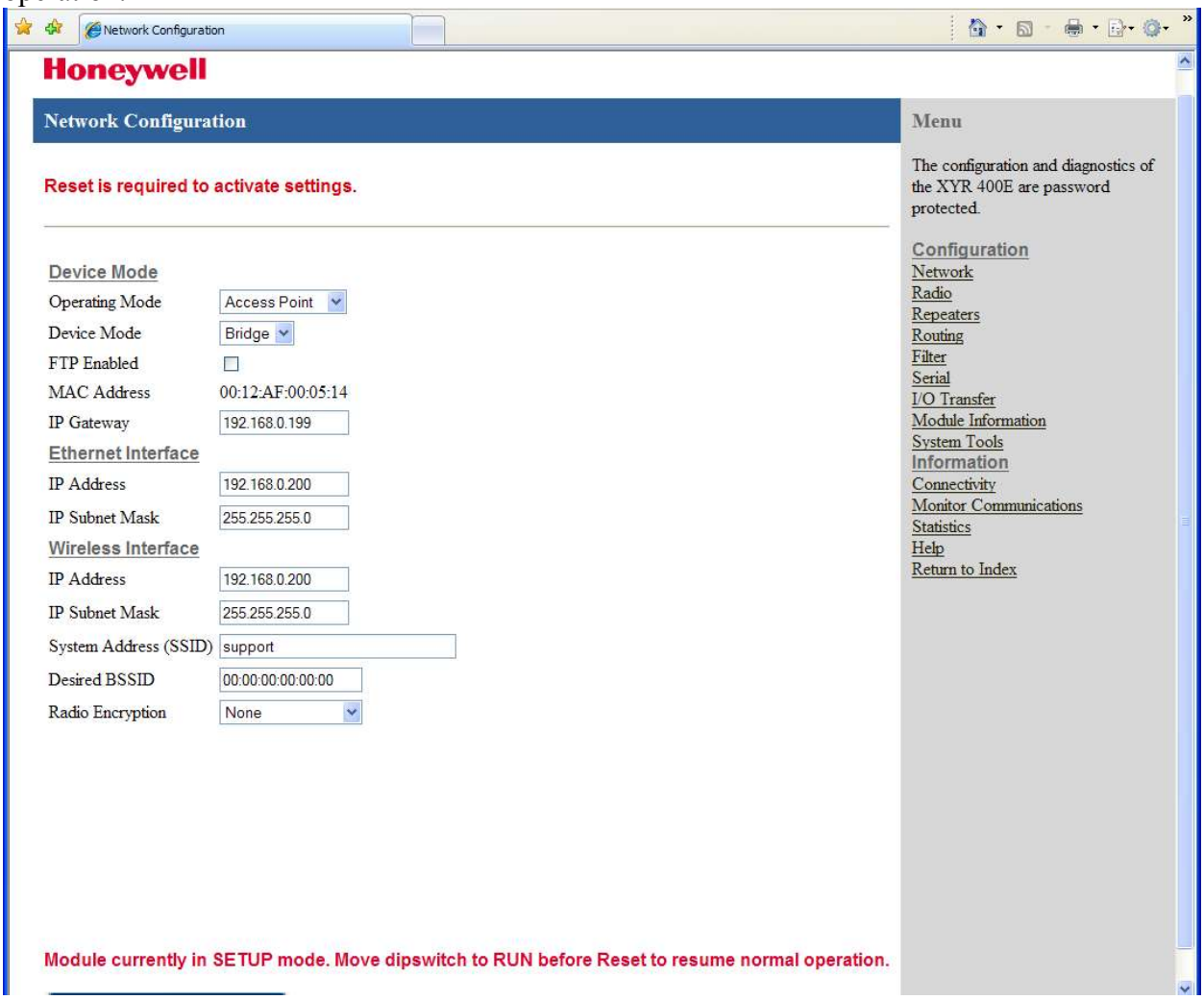
- Select Internet Protocol (TCP/IP) and click on Properties.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

- On the General tab enter IP address 192.168.0.1, Subnet mask 255.255.255.0, and default gateway 192.168.0.1.

- Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. If the PC uses a proxy server, ensure that Internet Explorer will bypass the Proxy Server for local addresses. This option may be modified by opening Tools -> Internet Options -> Connections Tab -> LAN Settings->Proxy Server -> bypass proxy for local addresses.
- Enter the default IP address for the XYR 400E *http://192.168.0.1XX* where XX is the last two digits of the serial number
- A welcome webpage should be displayed as illustrated below.
- Configuration and Diagnostics may be opened by clicking on any of the menu items, and entering the username "*user*" and default password "*user*". Configure the unit to your requirements (refer later sections of this manual).

When Configuration is complete, switch Factory Default dip-switch on XYR 400E to RUN position, and cycle power to resume normal configured operation.



3.4.2 Set XYR 400E to same network as PC

This is the alternate procedure to setting an IP address in the XYR 400E. Consult your network administrator for an IP address on your network, the gateway IP address, and network mask.

a) Switch Factory Default dip-switch on XYR 400E to SETUP position.

b) Connect the RS232 port on the XYR 400E to the RS232 port on the PC using a "straight-through" serial cable.

c) Open a terminal package (such as Hyperterminal) with 19200bps data rate, 8 data bit, 1 stop, no parity and no flow control. Make sure that no other programs have control of the serial port.

d) Power up XYR 400E. Basic network settings will be displayed on the terminal as illustrated below. When prompted, hit enter key to stop automatic boot process. You have 5 seconds to abort the boot process.

```
My Right Boot 2.1
 Copyright 1999-2004 Cybertec Pty Ltd, All rights reserved.
 This software is provided by Cybertec ``as is'' and with NO WARRANTY.
   http://www.cybertec.com.au/

ROM :   256KB @ 0xffe00000
RAM :  8192KB @ 0x00000000 (143KB / 0x00023d8c)

ROM Configuration table ... PASSED.
RAM address pattern check . PASSED.
RAM address bus check ..... PASSED.

Product       : E24g
Variant       : E2400-100
Serial No.    : 07050012 - 03061081212
Release       : epm_mrb_elpro_E24g_1.63
Released date : 1 March 2006
Released host : Anxosity
Build date    : Tue Mar  7 08:50:31 2006
Build host    : Anxosity
Boot Flags    : no RAM test, no ROM test, bus timer on, wdog on
                static IP, auto-boot, net-boot, reset on
                local file, no binary load
Boot delay    : 0
Boot Filename : /memory/0xffe40000,0x80000
Boot Address  : 192.168.0.112
Boot Netmask  : 255.255.255.0
Boot Gateway  : 192.168.0.1
Boot Host     : 192.168.0.220
Boot Mac 0    : 00:12:af:00:03:05
Boot Mac 1    : 00:12:af:00:03:05

RTE data store .... no error
Setting bus timer (on) and watchdog (on) ... PASSED

802.11 Interface Power ON...
Reset 802.11 Interface...
Checking 802.11 NIC (Base Address: 0x30000000)
Register Read-Write Test...OK
Initialising..Successful
Getting Serial Number..Reading Buffer..
Serial Number: 99SA01000000
Done..
Recovery Configuration :
ip address : 192.168.0.112
net mask   : 255.255.255.0
gateway    : 192.168.0.1
host       : 192.168.0.1

eip: mount point /memory
fec0: connected at 10M Half Duplex.
fec0: local ip = 192.168.0.112, server ip = 192.168.0.1

Press ENTER to abort automatic booting ... 5
```

e) Check values for Boot Address, Boot Netmask, and Boot Gateway. These values should be set to reflect those of the PC you are using to configure the unit. If these are correct skip to step (h). You may check settings again with the *rct* command. For further help, type the *help* command.

f) Set Boot Netmask to the same settings as the computer you have the Ethernet cable connected to. This may be performed with the command: *bnm <Type the netmask>*

g) Set Boot Gateway to the same settings as the computer you have the Ethernet cable connected to. This may be performed with the command: *bgw <Type the gateway IP address>*

h) Choose an IP address for the XYR 400E being upgraded. This IP address must be on the same network as the computer you have connected the Ethernet cable to. This may be performed with the command: *bip <Type the IP address>*

i) Switch dip-switch on XYR 400E to RUN position.

j) Type the command *reset*, or cycle power to the unit. The XYR 400EE will reset and start with the network settings you have entered.

k) Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. If the PC uses a proxy server, ensure that Internet Explorer will bypass the Proxy Server for local addresses. This option may be modified by opening Tools -> Internet Options -> Connections Tab -> LAN Settings->Proxy Server -> bypass proxy for local addresses.

l) Enter the webpage *http://xxx.xxx.xxx.xxx/* where *xxx.xxx.xxx.xxx* is the IP address selected for the module. A welcome webpage should be displayed as illustrated.

m) Clicking on any of the menu items, and entering the username "user" and password "user" may open Configuration and Diagnostics. If the password has previously been configured other than the default password, then enter this instead.

3.5 Network Configuration

You can view or modify Ethernet network parameters by selecting the "Network" menu. When prompted for username and password, enter "user" as the username, and "user" as the password in the password field. If IP address or password has been forgotten, the Factory Default switch may be used to access the existing configuration. Refer to section 3.3 above.

The Network Configuration page allows configuration of parameters related to the wired and wireless Ethernet interfaces. In general, IP address selection will be dependant upon the connected wired Ethernet device(s) – before connecting to an existing LAN consult the network administrator.

A system of XYR 400E's must have at least one Access Point acting as a master to one or more Clients. All XYR 400E's to be configured as part of the same wireless network should be given the same System Address (SSID) and Radio Encryption settings. For further information and examples on wireless network topologies refer section 1.1 above.

The XYR 400E supports several different radio encryption schemes. WEP (*Wired Equivalent Privacy*) encryption is the weakest encryption method, defined by the original IEEE802.11 standard. 64bit and 128bit WEP combine either a 40bit or 104bit key with a 24bit initialization vector, and are intended to provide equivalent security attributes to those of a wired medium. The XYR 400E supports both 64bit and 128bit WEP without any performance (throughput) degradation.

WPA (*WiFi Protected Access*) is a subset of the IEEE802.11i Security Enhancements specification. The XYR 400E supports WPA-1 TKIP and WPA-2 AES using a *Pre-Shared Key* (PSK). TKIP (*Temporal Key Integrity Protocol*) enhances WEP by using 128bit encryption plus separate 64bit Tx and Rx MIC (*Message Integrity Check*) keys. Enabling TKIP will degrade the XYR 400E radio throughput by approximately half of the rate attainable using either WEP or no encryption. AES (*Advanced Encryption Standard*), the most secure encryption method, is also based on 128 bit encryption key. Enabling AES in the XYR 400E will degrade radio throughput to approximately 20% of the rate attainable using either WEP or no encryption.

After changes are made to Network Configuration, it is important to save the configuration by selecting "Save and Reset".

Network Settings Webpage Fields

Operating Mode	Used to select Access Point (Infrastructure), Client (Infrastructure), IBSS (Ad-Hoc), or MONITOR mode. By default this is set to Client.
Device Mode	Used to select Bridge or Router mode. By default this is set to Bridge.
FTP Enabled	This enables access to volatile memory storage on the XYR 400E. By default this is disabled.
MAC Address	This is the unique hardware address of the XYR 400E, assigned in the Factory. For the majority of systems, this item should not be changed. If the device is to be connected to equipment that will only communicate with a set MAC Address, the XYR 400E may clone that MAC address.
Gateway IP Address	This is only required if the wired LAN has a Gateway unit which connects to devices beyond the LAN - for example, Internet access. If there is no Gateway on the LAN, set to the same address as the Access Point - that is, the "Ethernet IP Address" below.
Ethernet IP Address	The IP address of the XYR 400E on its wired Ethernet port. This should be set to the IP address you require.
Ethernet IP Subnet Mask	The IP network mask of the XYR 400E on its Ethernet port. This should be set to the IP address you require.
Wireless IP Address	The IP address of the XYR 400E on the wireless port. If the unit is configured as a bridge this address will be the same as the Ethernet IP address. If configured as a router, the IP address must be different from the Ethernet IP Address - it must be consistent with the LAN it is connecting to on the wired side.
Wireless IP Subnet Mask	The network mask of the XYR 400E on the radio port. If configured as a Bridge, this must be the same as the Ethernet IP Subnet Mask.
System Address (SSID)	A XYR 400E network comprises modules with the same "system address". Only modules with the same system address will communicate with each other. The system address is a text string 1 to 31 characters in length. Select a text string which identifies for your system.
Desired BSSID	To force a client/station to always connect to the same Access Point enter the MAC address of that Access Point in the Desired BSSID field (Note that the SSID of the Access Point must also match the configured SSID of the client).
Radio Encryption	Select "None", "WEP (64-bit)", "WEP (128-bit)",

	"WPA-PSK (TKIP)", or "WPA-PSK (AES)" security encryption of the wireless data. The default setting is "None".
Encryption Keys 1 to 4	These are the keys used to encrypt radio data to protect data from unwanted eavesdroppers when WEP Encryption is selected. These keys should be the same for all XYR 400E units in the same system. One of the four keys may be selected as the default key, and is used to encrypt transmitted messages from the configured unit. A XYR 400E can receive and decrypt a message from a module that has a different default key index as long as each module has the same key configured at the same index. WEP keys must be entered as pairs of hexadecimal digits separated by colons. Hexadecimal digits are in the range 0..9 and A..F. 64bit WEP requires 10 Hexadecimal digits, and 128bit WEP requires 26 Hexadecimal digits. For example, 12:AB:EF:00:56. for 64bit encryption, and 12:AB:EF:00:56:15:6B:E4:30:C8:05:F0:8D for 128bit encryption Encryption keys must not be all zeros, i.e. 00:00:00:00:00
Passphrase	When WPA Encryption is selected, 128bit Encryption keys are internally generated based on the Passphrase and System Address (SSID). The Passphrase must be between 8 and 63 characters in length, and the Passphrase must be the same for all XYR 400E units in the same system.
Save and Reboot.	Save settings to non-volatile memory, and reboot XYR 400E.

3.6 Ethernet Data

All Ethernet devices are uniquely identified by a MAC Address that identifies the hardware device. These addresses are factory-set and are six bytes in size and are expressed in hexadecimal in the form *xx:xx:xx:xx:xx:xx*

Ethernet messages can be addressed to a single device (a point-to-point message) or can be directed towards multiple destinations by using Multicast addresses and Broadcast addresses. The broadcast address is used to send data to all devices. The broadcast address is FF:FF:FF:FF:FF:FF.

Multicast addresses are used to direct data at a set of devices. Multicast addresses may be recognized as they are always have the least significant bit of the first byte of the MAC Address set. For example, 0**1**:00:5E:00:00:00 is a multicast address, 0**1**:80:C2:00:00:00 is also a multicast address.

3.7 Normal Operation

After addresses are configured, the units are ready for operation.

Refer to section 1 for an explanation on the operation of a Bridge and Router.

Transparent Bridge Operation

Bridges are typically used to connect sections of the same IP network together.

By default, the XYR 400E is configured as a transparent bridge. When a transparent bridge is started, it learns the location of other devices by monitoring the source address of all incoming traffic. Initially it forwards all traffic between the wired Ethernet port and the wireless port, however by keeping a list of devices heard on each port, the transparent bridge can decide which traffic must be forwarded between ports - it will only transfer a message from the wired port to the wireless port if it is required.

A bridge will forward all Broadcast traffic between the wired and wireless ports. If the wired network is busy with broadcast traffic, the radio network on the XYR 400E can be unnecessarily overburdened. Filtering may be used to reduce broadcast traffic sent over the radio. Refer Section 3.12 for how to configure a filter.

By default, a transparent bridge does not handle loops within the network. There must be a single path to each device on the network. Loops in the network will cause the same data to be continually passed around that loop. Redundant wireless links may be set up by enabling the bridge Spanning Tree Protocol (see section "3.9 Spanning Tree Protocol" for more details).

3 or 4 Address Mode

There are two different operating modes that affect bridge operation for a XYR 400E client/station – "3-Address Mode" or "4-Address Mode".

> "3-address mode" *must* be used by XYR 400E clients when they have to communicate with third party (non-XYR 400E) Access Points.

However, "4-address mode" (which is also used for multiple Access Point Repeaters), may be used by XYR 400E clients when they communicate with other XYR 400E Access Points. Address mode configuration can be altered via the *Repeaters* configuration page.

When 3-address mode is used it is not possible for a XYR 400E client to transmit over the radio link the MAC address of any device connected to its wired Ethernet port. Therefore, the XYR 400E client must act as a proxy for devices lying on its wired Ethernet port, and use its own MAC address on their behalf. To do this, it analyzes the IP addresses within the Ethernet frame body and builds a lookup table so that when radio traffic is received it can lookup the device MAC address based on its IP address. This functionality is referred to as *Layer 3 Bridge*. Note that because the layer 3 bridge relies on IP, it is only suitable for bridging Ethernet frames from devices that communicate using IP. For this reason the bridge Spanning Tree Protocol can *not* be used with 3-address mode. When a XYR 400E client/station uses 3-address mode any Access Point that it is to communicate with may be configured for *either* 3 or 4 address mode (i.e. Access Point mode does not matter).

4-address mode allows a XYR 400E client/station to bridge traffic from devices connected to its wired Ethernet port without acting as a proxy for their MAC address. This means that a XYR 400E client/station in 4-address mode can bridge *any* Ethernet traffic – not just IP based traffic as with 3-

address mode. 4-address mode should also be used if the bridge Spanning Tree Protocol is required. When a XYR 400E client/station uses 4-address mode any Access Point that it is to communicate with *must* also be configured for 4-address mode.

Router Operation

A router joins separate Ethernet networks together. The router has different IP addresses on its wired and wireless ports, reflecting the different IP addresses of the separate Ethernet networks. All the devices in the separate networks identify the router by IP address as their gateway to the other network. When devices on one network wish to communicate with devices on the other network, they direct their packets at the router for forwarding.

As the router has an IP address on each of the networks it joins, it inherently knows the packet identity. If the traffic directed at the router can not be identified for any of the networks to which it is connected, the router must consult its routing rules as to where to direct the traffic to. For details on configuring routing rules see section "3.11 Routing Rules".

3.8 Radio Configuration

The XYR 400E can be configured for different radio transmission rates. A reduction in rate increases the reliable range (transmission distance). The factory-default data rate settings are suitable for the majority of applications and should only be modified by experienced users.

The XYR 400E allows for configurable *fixed* or *fallback* radio transmission Data Rates. When a fixed rate is configured the radio transmission rate is never altered, even under extremely poor conditions. The fallback rates allow a maximum rate to be configured whilst enabling the unit to automatically reduce the rate when transmit errors occur. When a radio transmission is unsuccessful the XYR 400E will automatically drop to the next lowest data rate and enter *probation*. If subsequent transmissions are successful at the lower rate, the XYR 400E will attempt to increase to the next highest rate when probation has ended. This can occur when either a specified number of data frames have been successfully transmitted at the lower rate, or when a specified amount of time has elapsed whilst using the lower rate.

The XYR 400E also has a configurable "Basic Rate". The difference between the Basic Rate and the radio Data Rate is that it only applies to multicast radio transmissions and *management* frames. The Basic Rate is generally set to a lower value than the Data Rate since multicast transmissions have no inherent error correction mechanism.

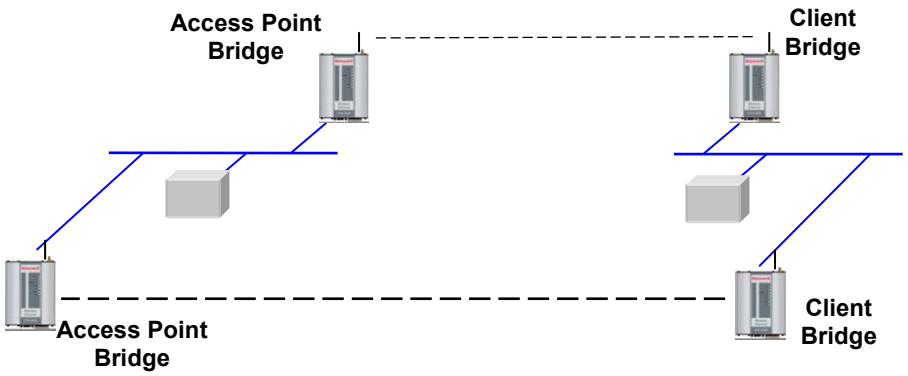
Select the "Radio" Menu to change the following configuration parameters. If a change is made, you need to select "Save Changes" to retain the changes. Changes will not take effect until the unit is reset.

Power Level	The RF power level is shown in this field. This value is read only and cannot be altered.
Data Rate	The radio baud rate in Mega (million) bits per second (Mbps) for point to point radio transmissions. The default value is Auto.
Basic Rate	The radio baud rate in Mega (million) bits per second (Mbps) for multicast messages and management frames. These frames include beacons, authentication, association, etc. The default value is 2Mbps.
Channel	Radio Channels 1 to 11 may be configured at the Access Point. Refer Section 3.2. By default radio channel is set to 3.
Beacon Interval	This interval is the period between beacon transmissions sent by an Access Point. The default value is 100 milliseconds, and it may be adjusted from 50 to 4095 milliseconds.
RTS Threshold	RTS frames can be used to help avoid radio collisions between two stations that cannot directly hear each other. Any frame larger than RTS Threshold bytes will be preceded by an RTS message.
Fragmentation Threshold	STA only. The maximum transmission unit (MTU) of data over the radio. If more than this number of bytes is input into the module, it will be transmitted in more than one message (or fragment).
Fallback Probation Counter	When one of the fallback data rates is selected, the radio data rate may be upgraded to the next highest rate after this many consecutive successful transmissions. The default value is 10.
Fallback Probation Timer	When one of the fallback data rates is selected, the radio data rate may be upgraded to the next highest rate after this amount of time is spent at a lower rate. The default value is 20 seconds.
Disable SSID broadcast.	This should be used to prevent unwanted eavesdroppers from detecting the radio network System Address (SSID) by passively listening to beacon transmissions from the Access Point. When disabled, Access Points will not transmit the System Address openly in Beacon messages. This is particularly useful in unencrypted radio networks.
Disallow Probe Requests without correct SSID	This should be used to prevent unwanted users from detecting the radio network System Address (SSID) actively by sending a probe request to the Access Point. When Disallowed, if the correct System Address is not supplied in the probe request, the Access Point will not respond. This is particularly useful in unencrypted radio networks.
Save Changes	Save changes to non-volatile memory. Changes will not take effect until module is reset.
Save Changes and Reset	Save changes to non-volatile memory and reset module

3.9 Spanning Tree Algorithm / Redundancy

The bridge "Spanning Tree Protocol" function was introduced to handle network loops and provide redundant paths in networks. To enable the STP requires that WDS mode also be enabled on the "Repeaters" configuration page. When enabling WDS mode on a client/station you should ensure that WDS mode is also enabled at the corresponding Access Point – refer section 3.10 for more information.

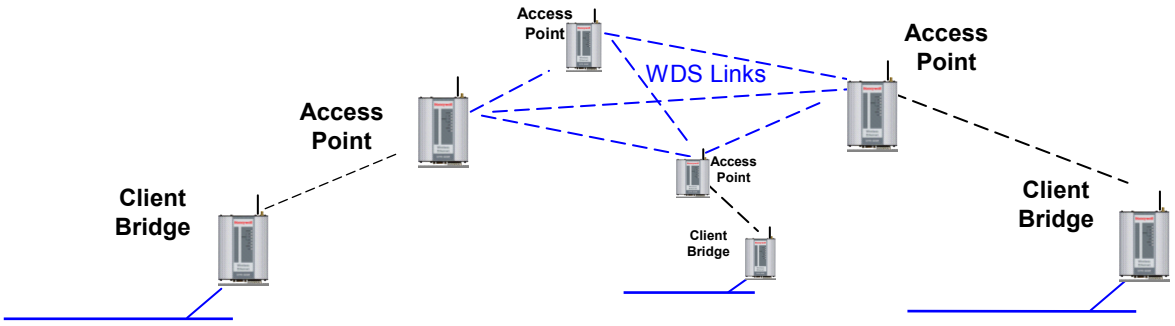
For example, consider this network with a redundant wireless link. If the bridge Spanning Tree Protocol is enabled, one of the two wireless links will be disabled - that is, all wireless data will be transferred by one link only. If the active link fails, the other link will automatically start transferring the wireless data.



The Spanning Tree Protocol implemented is IEEE 802.1d compatible. The algorithm forms a loop-free network by blocking traffic between redundant links in the network. These blocked links are placed in a standby condition, and may be automatically enabled to repair the network if another link is lost. The Spanning Tree Algorithm maintains a single path between all nodes in a network, by forming a tree-like structure. The Bridge Priority determines where the node sits in the tree. A Bridge configured with the lowest priority (0) will become the root node in the network, and will direct traffic between each of its branches. The root node is typically the unit that handles the majority of traffic in the network. The XYR 400E is configured with a Bridge Priority of 32768 by default. The intention is to reduce traffic that the XYR 400E must handle, by placing it at the branch level in the network tree. As a branch, the XYR 400E needs only pass traffic to devices that are its "leaves".

There is some overhead in maintaining a network utilizing the Spanning Tree Algorithm. Users wishing to increase their throughput, at the expense of redundancy should disable Spanning Tree. The Spanning Tree Protocol can be configured on the *Repeaters* configuration page – note that 4-address mode *must* be enabled if the bridge Spanning Tree Protocol is to be used (refer section "3.7 Normal Operation" for details).

3.10 Multiple AP Repeater Mesh Network



The range of a wireless network can be extended by allowing Access Points to behave as repeaters and forward traffic to other Access Points. Access Point to Access Point communications is also known as Wireless Distribution System (WDS). The XYR 400E offers very powerful WDS configuration, allowing for a *mesh* network with self-healing and automatic node discovery. Alternatively, fixed AP to AP links can be configured for optimized throughput.

WDS Access Points require IEEE802.11 4-address mode. 4-address mode may also be used by XYR 400E clients when Ethernet protocols other than IP are to be used – see section "3.7 Normal Operation" for more details.

Each XYR 400E Access Point supports up to 6 separate *interfaces* for WDS links to other Access Points. Each WDS interface can be either a *bridge* or *router* interface (refer section "1.1 Network Topology" for more information on bridge vs router). If you need a simple repeater network, use a bridge interface.

A WDS *bridge* interface allows traffic to be bridged to another Access Point on the same IP network. WDS bridge interfaces do not require additional IP Address configuration, as they are bridged with the standard *wireless interface* that is used for connections to associated clients. All 6 WDS interfaces on the one Access Point may be bridged if required.

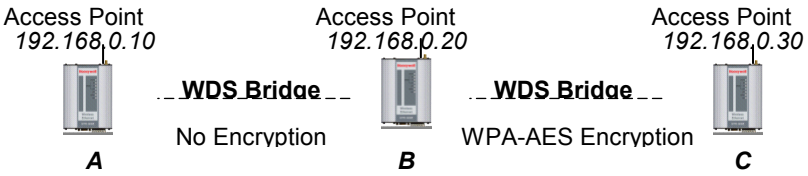
WDS bridge interfaces have the advantage that redundant paths are permitted when using the bridge Spanning Tree Protocol (see section "3.9 Spanning Tree Protocol"), thus behaving as a self-healing mesh network. Bridged networks are also not as configuration intensive as routed networks. Since WDS bridge interfaces generally do not require IP address configuration (they inherit the IP address of the standard wireless interface), they can be configured to automatically connect to other WDS enabled Access Points.

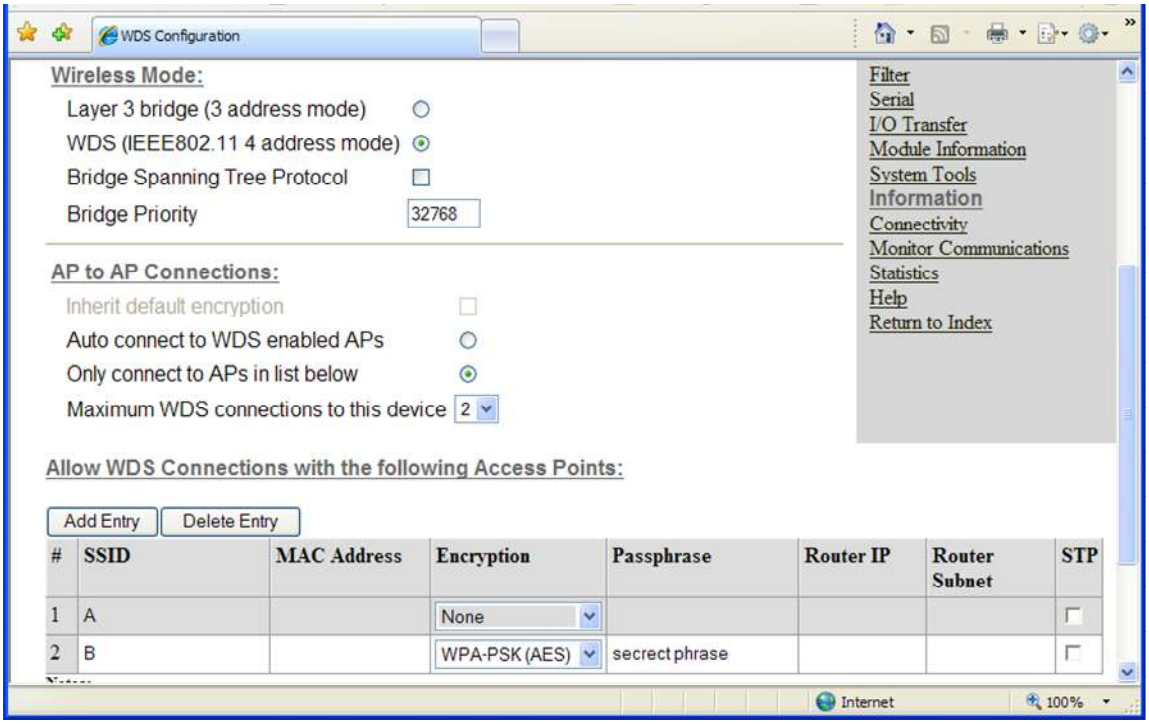
A WDS *router* interface allows traffic to be routed to an Access Point on a different network, and therefore requires configuration of an IP address to reflect the network address of the destination network. WDS router interfaces cannot provide the redundancy of bridge interfaces, but can be used to reduce radio bandwidth requirements because the router can determine the destination based on IP address, whereas the bridge must go through a learning phase where all broadcast traffic must be retransmitted on each interface. Routed networks may also be used in some cases to avoid the overhead introduced by the bridge Spanning Tree Protocol when network loops exist.

Each WDS interface may also be configured with a different encryption algorithm; however each side of a WDS link must specify the same encryption algorithm and keys. When configuring a mesh (i.e. auto connect) network with encryption, the same encryption algorithm and keys must be

inherited from the default interface. Note that when WPA is required with a mesh network, the same SSID must be used for each Access Point. Alternatively the list of possible allowed Access Points (by SSID) and their corresponding passphrases must be specified - since WPA Pre-Shared Keys are derived from both passphrase *and* SSID. WEP encryption can only be used for a WDS link when WEP has also been enabled for the default wireless interface, the default WEP key will also be inherited.

One of the most common uses for WDS is to extend the range of the wireless network using repeaters. The diagram below illustrates a simple example where the three Access Points are all at fixed locations (each of the Access Points could, of course, have one or more client/stations connected). Since the locations are fixed, we can avoid the overhead of using the Bridge Spanning Tree protocol here by configuring fixed WDS links to ensure that each Access Point will only connect to the next Access Point in the chain. Any number of additional intermediate repeaters could be added to the chain in a similar way.

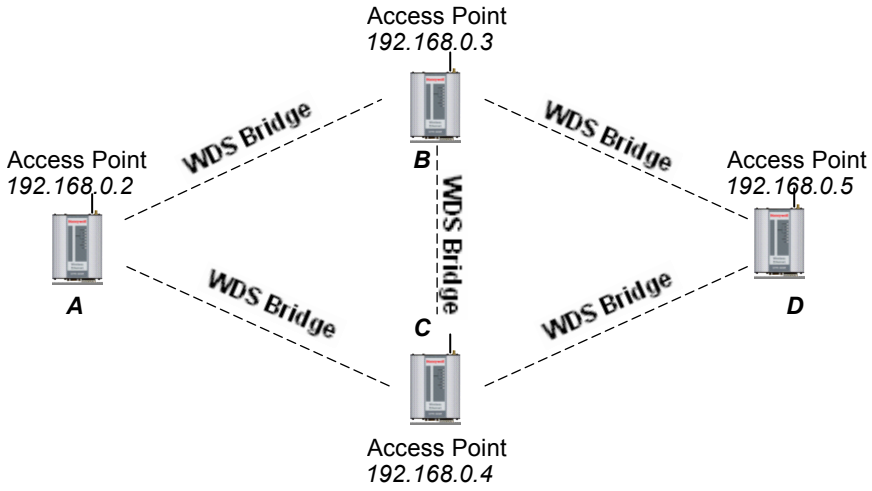




The WDS configuration for unit B is shown above (this page is accessible via the *Repeaters* link from the configuration web pages). WDS mode has been enabled, and "Only connect to APs in list" has been selected so that the repeater path is fixed. Since this example is a bridged network (i.e. all devices on the same IP network) and there is no possibility of loops (i.e. multiple paths to the same location) we do not need to incur the overhead of enabling bridge spanning tree protocol. It can be seen that there are 2 entries in the WDS connections list for unit B. We specify the Access Points at the other end of the WDS links by SSID only – though MAC addresses could also have been

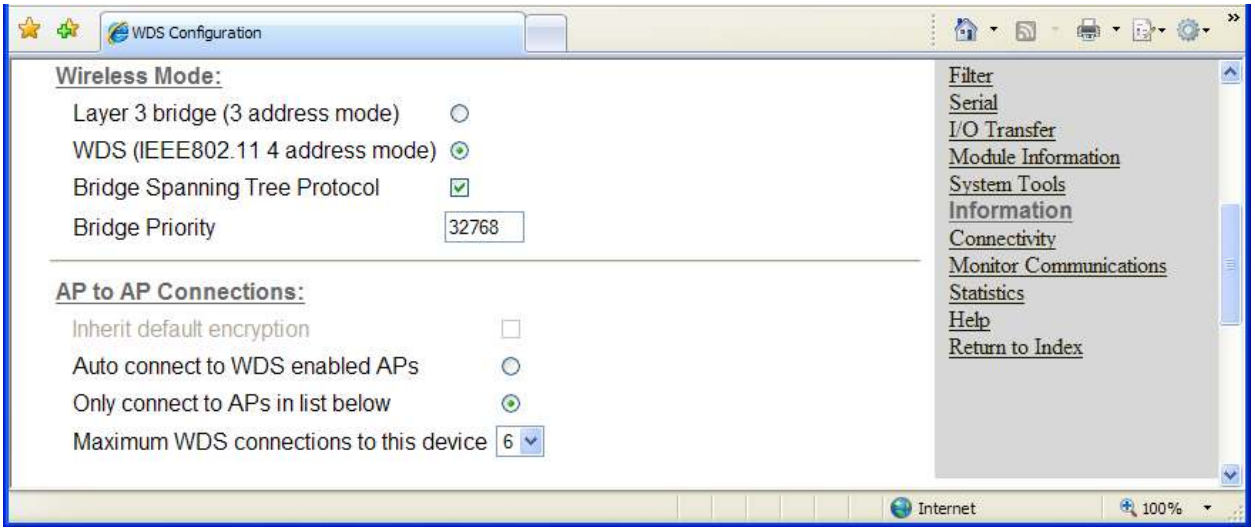
specified if there are multiple Access Points with the same SSID. Finally, in this example we demonstrate the flexibility of the XYR 400E by specifying different Encryption on only one of the WDS links.

In the example below, 4 Access Points (A, B, C, and D) form a mesh network using only WDS bridge interfaces. Each of the Access Points may also have its own clients associated. Each Access Point also has the same SSID, meaning the clients can roam freely throughout the mesh network and also that WPA encryption may easily be used. A, B, C, and D can all exchange data with each other (as can all of their clients) as if they were all on the same wired segment. It can bee seen that there are redundant paths and therefore the possibility for loops to occur, so that the bridge Spanning Tree Protocol should be enabled. To illustrate the redundancy, consider that if A needs to send data to D it has redundant paths through both B and C. However, due to the spanning tree protocol only one of B or C will relay the data, with the other taking over in the event of a failure.

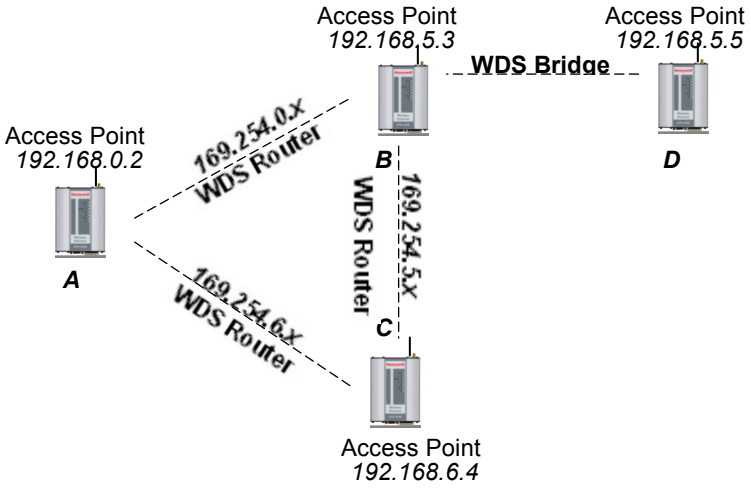


The configuration for unit A is shown below (this page is accessible via the *Repeaters* link from the configuration web pages). It can be seen that "WDS" mode and "Bridge Spanning Tree Protocol" are enabled, and "Auto Connect to WDS enabled AP's" is selected. Note that auto connect mode requires that none of the Access Points disable their "SSID broadcast", otherwise they must have the same SSID. If this is not the case the connections must be manually entered into the WDS connection list (described later).

"Inherit default encryption" has also been selected – thus allowing us to inherit the same encryption mode used for the default wireless interface (i.e. the interface used to communicate with clients). If WPA encryption is inherited, then all Access Points must have the same SSID otherwise the list of possible allowed Access Points (by SSID) and their corresponding passphrases must be specified in the connection list since WPA Pre-Shared Keys are derived from both passphrase *and* SSID.

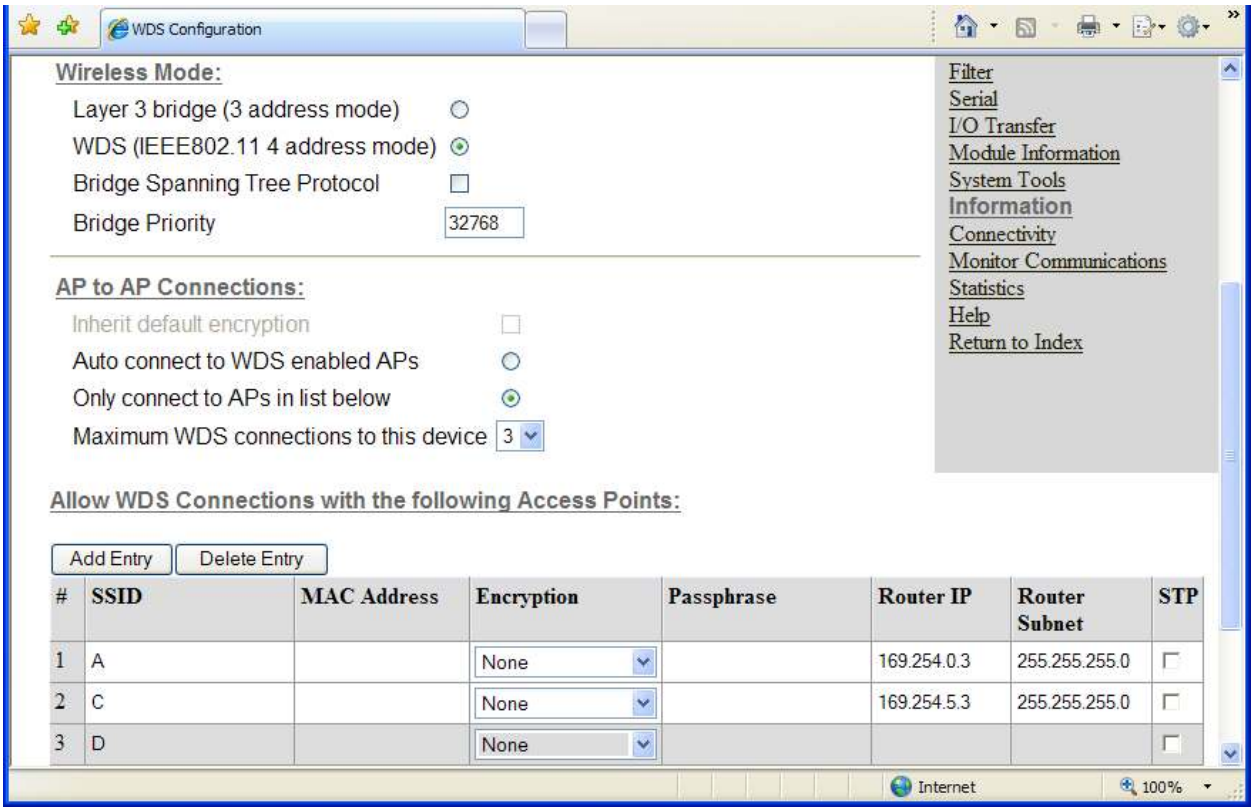


An example of using WDS router interfaces to achieve a similar physical topology to the WDS bridge example discussed earlier is illustrated below. In both examples, there are four WDS Access points each with the possibility of having their own client/stations associated. In both examples A, B, C, and D can all exchange data with each other. The bridged example has the advantage of redundancy but at the expense of extra overhead. The routed example below cannot provide the redundancy of the bridged example, and requires more configuration effort, but does not have the overhead of using the bridge Spanning Tree Protocol, so is suited to fixed installations that do not require redundancy.



As mentioned previously, configuration of the WDS router example is more complex than the bridged example given earlier. In this case, all Access Points have different SSID's and none of them have SSID broadcast disabled so that WDS configurations can be made without knowledge of Access Point MAC addresses. If SSID broadcasts were disabled, each configuration entry would require an SSID *and* a MAC address (this is because both SSID *and* MAC addresses are required to establish a link – but the MAC address is always broadcast in beacons whereas the SSID broadcast is configurable).

Unit B in the WDS router example above has three WDS links – to units A, C, and D; we show unit B's configuration below. It can be seen that there are 3 entries in the WDS Connections list. The first entry specifies a connection to the Access Point whose SSID is "A", and that it is to be a WDS router interface with Router IP address 169.254.0.3 (this is the address that unit B adopts for the router interface link to unit A). Note that this IP Address specifies a different network than that of the default interface for unit B (i.e. default interface network 192.168.0.x compared to WDS interface network 169.254.0.x). It is a requirement that the interfaces at each end-point of a WDS link have the same *network* address, so by using a different network address to that of the default interface we ensure that each end point has a different network address than its default interface. This ensures that the WDS links at either end point are not bridged with their default interface, since in this example we wish to eliminate the overhead associated with a bridged interface.

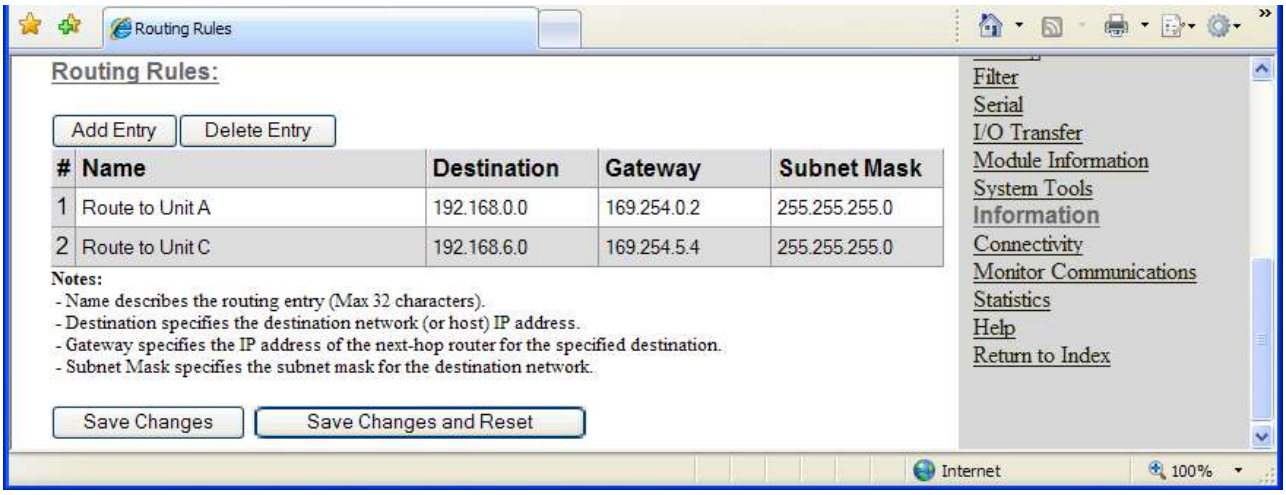


A consequence of using a different network address for the WDS link between unit A and B, is that we now need to configure a *routing rule* at units A and B so that the XYR 400E can determine where to send traffic destined for the respective network addresses of A and B. For example, if unit B receives traffic destined for network 192.168.0.x (i.e. somewhere on unit A's network), the routing rule specifies that the traffic must be forwarded to the end point of the WDS link to unit A. The routing rules for unit B are shown below (for more information on routing rules, refer to the section "3.11 Routing Rules").

The second WDS entry above specifies the WDS link to unit C as a WDS router interface with IP address 169.254.5.3. As with the WDS link to unit A, we use a different IP network address than the default interface (note that this network address 169.254.5.x is also different to that used for the WDS link to unit A 169.254.0.x, so that these separate WDS interfaces are not internally bridged). Also, as with the WDS link to unit A, a routing rule is added to direct traffic destined for the network address of unit C (192.168.6.x). So, in this example, unit B has a total of three IP

addresses: 192.168.5.3 for the default interface; 169.254.0.3 for the WDS link to unit A; and 169.254.5.3 for the WDS link to unit C. Note that we choose to always use the same *host* address of 3 for unit B on all of its interfaces regardless of the network address.

The third WDS entry above specifies the WDS link to unit D. In the example unit D has the same network address as unit B, therefore we wish to have the WDS interface link to unit D bridged with the default interface. Because we don't specify a router IP address for the third entry the XYR 400E automatically bridges this interface with the default wireless interface.



The routing rules for unit B are shown above. The routing rule for directing traffic to unit A can be seen to specify 192.168.0.0 as the destination address (the *network* address of unit A) – because the last byte is zero, this refers to a route to the *network* 192.168.0.x (as opposed to a route to an individual *host*). The same rule specifies the address 169.254.0.2 as the gateway address (this is the WDS Router IP address that unit A has been configured with for its WDS link to unit B). So, this routing rule effectively tells the XYR 400E that any traffic destined for the network 192.168.0.x should be forwarded to unit A via the WDS link. Units A and C would also require similar pairs of routing rules to direct traffic to the network addresses at the end points of their respective WDS links. For unit D it would suffice to simply configure unit B as its default gateway, as unit B would then forward on any traffic destined for units A and C. Refer to section "3.11 Routing Rules" for further information on routing rules.

The WDS Configuration page (as seen above) is accessible from the "Repeaters" link on any of the configuration web pages. The configurable WDS parameters are summarized below.

Layer 3 bridge	When WDS communications are not required, select this option (see section "3.7 Normal Operation" for details on Layer 3 bridge).
WDS	Select WDS to enable Access Point to Access Point communications.
Bridge Spanning Tree Protocol	Select this to enable Bridge Spanning Tree Protocol when the default radio interface is bridged (see section "3.9 Spanning Tree Protocol").
Bridge Priority	The bridge priority when the Spanning Tree Algorithm is enabled. Defaults to 32768 with minimum of 0 (highest priority), maximum of 65535 (lowest priority).
Auto connect to WDS	Attempt to automatically establish WDS links with other Access Points –

Enable AP's	even if those Access Points are not present in the list (NOTE – requires that Access Points that are not in the list do *not* have "SSID broadcast" disabled, otherwise the SSID is assumed to be the same as this Access Point; Auto connect interfaces will always be bridged with the default wireless interface).
Only connect to AP's in list	Only attempt to establish WDS links with Access Points identified in the list.
Maximum WDS connections to this device	Each XYR 400E Access Point supports a maximum of 6 WDS links direct to other Access Points. However the maximum may be reduced – this can be useful when Auto Connect is used.

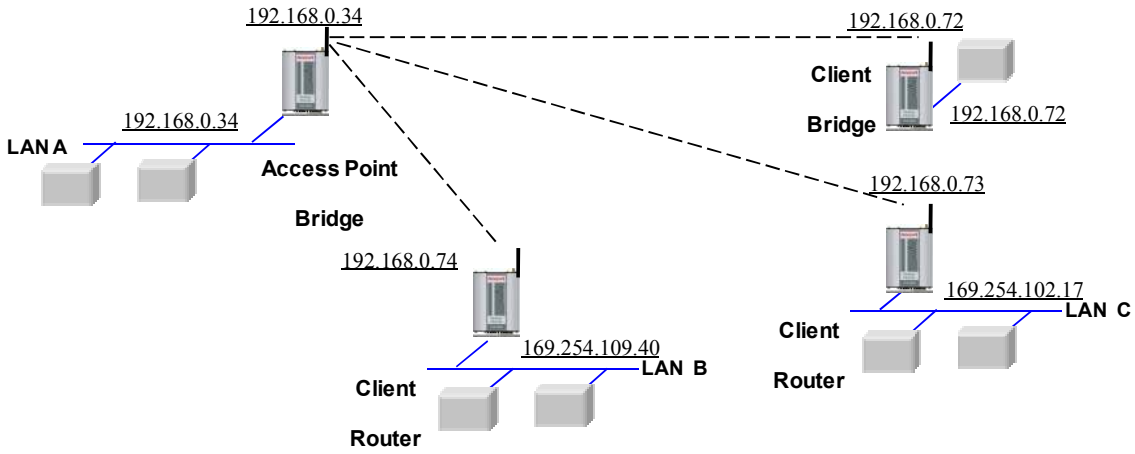
WDS Connections:

SSID	Specify the SSID of the Access Point(s) to establish a WDS link with. Leave this field blank if you wish to nominate the Access Point by MAC address only – however in that case the Access Point must *not* have "SSID broadcast" disabled.
MAC Address	Specify the MAC address of an Access Point to establish a WDS link with. Leave this field blank if you wish to connect to *any* Access Point with the nominated SSID
Encryption	Select the required Encryption (if any) for this WDS link. If WEP Encryption is required WEP must also be enabled for the default wireless interface – and the same WEP key will be inherited.
Passphrase	When WPA Encryption is selected, enter the WPA passphrase for this WDS link here.
Router IP	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise enter the IP address for *this* Access Point that specifies the IP network to route messages to.
Router Subnet	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise enter the subnet mask of the network to route messages to.
STP	Applicable to WDS Router interfaces only. If two or more WDS router interfaces having the same Router IP Address and Subnet mask become active the XYR 400E must internally bridge them. Select the STP option if you wish to enable the bridge Spanning Tree Protocol for the bridge if this interface is added.

3.11 Routing Rules

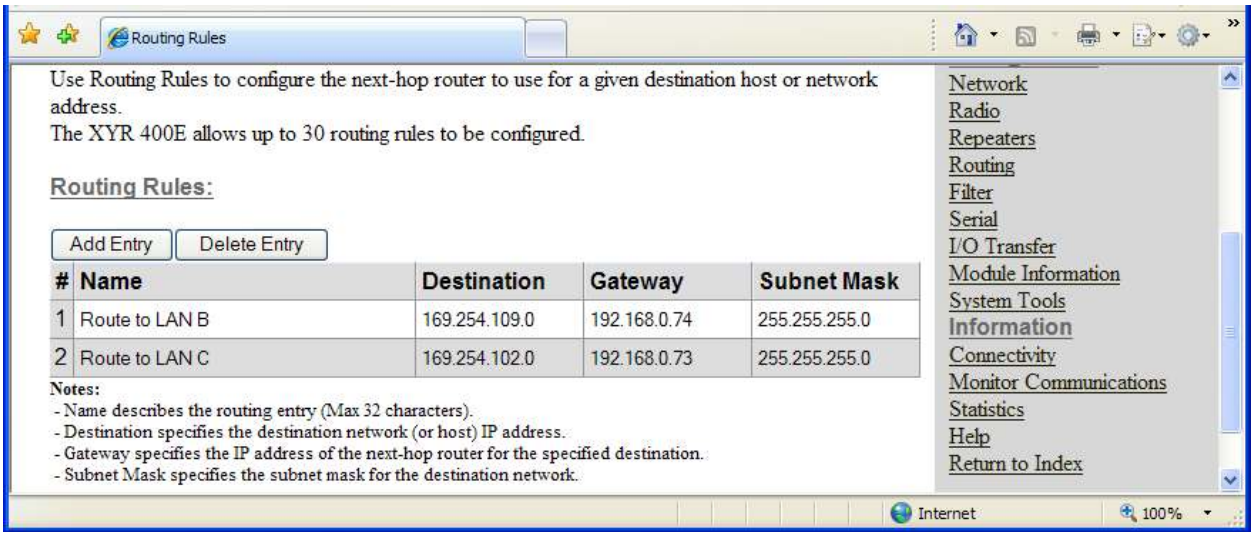
When a XYR 400E receives an IP frame that is destined for an IP address on a different network, it checks if the network address matches the network address of one of its own interfaces (i.e. hard wired Ethernet, or wireless Ethernet, or WDS) and forwards the frame appropriately. However, if the IP network address does not match any of its interfaces, the XYR 400E will forward the frame to its default gateway. In this case it is assumed that the default gateway has a valid route to the destination.

In some cases it is not practical to have just one default gateway (i.e. routed wireless networks with more than two XYR 400E routers; and in some cases when WDS router interfaces are used). If more than one "next-hop router" is required, the XYR 400E allows for up to 30 *routing rules* to be configured. A routing rule specifies a destination network (or host) IP address and the corresponding next-hop router that messages for the specified destination will be forwarded to. It is assumed that the next-hop router (or *gateway*) will then deliver the data to the required destination (or forward it on to another router that will).



The above network diagram illustrates a situation where routing rules may need to be configured. In this example, the XYR 400E clients need only specify the Access Point as their default gateway (i.e. they require no routing rules be configured). However, for the Access Point to be able to deliver traffic to LAN B and LAN C it needs to have routing rules configured that specify the respective XYR 400E client/routers as next-hop routers (i.e. gateways) to networks B and C. Note that devices on LAN A should specify the XYR 400E Access Point as their default gateway. An alternative to adding routing rules to the XYR 400E in this example would be for each device on LAN A that needs to communicate with LANs B and C to independently have routing rules specifying the XYR 400E clients at B and C as gateways to those networks.

The routing rules for the Access Point in the above example are shown below. The first entry shows the route to LAN B. The gateway for the route to LAN B is configured as the wireless IP address of the XYR 400E client connected to LAN B. The destination for the route is configured as the *network* address of LAN B. Because the *host* id of the destination IP address is 0, it specifies a network address. Consequently, any traffic received at the Access Point with destination IP address 169.254.109.x (where x is any host id) will be forwarded to the XYR 400E at LAN B.


Routing Rules
Use Routing Rules to configure the next-hop router to use for a given destination host or network address.
The XYR 400E allows up to 30 routing rules to be configured.
Routing Rules:
Add Entry
Delete Entry
Name Destination Gateway Subnet Mask
1 Route to LAN B 169.254.109.0 192.168.0.74 255.255.255.0
2 Route to LAN C 169.254.102.0 192.168.0.73 255.255.255.0
Notes:
- Name describes the routing entry (Max 32 characters).
- Destination specifies the destination network (or host) IP address.
- Gateway specifies the IP address of the next-hop router for the specified destination.
- Subnet Mask specifies the subnet mask for the destination network.
Network
Radio
Repeaters
Routing
Filter
Serial
I/O Transfer
Module Information
System Tools
Information
Connectivity
Monitor Communications
Statistics
Help
Return to Index
Internet
100%

The Routing Rules configuration page can be accessed by selecting the "Routing" link on any of the configuration web pages. Up to 30 routing rules may be added to each XYR 400E. The table below summarizes the configurable parameters of a routing rule.

Name	A name to describe the routing rule (Max 32 characters).
Destination	The destination network (or host) IP address (to specify a network address set the host address to 0. i.e. for a class C IP address 192.168.0.0 would specify a destination network, while 192.168.0.16 specifies a destination host).
Gateway	The IP address of the next-hop router for the specified destination.
Subnet Mask	The subnet mask for the destination network.

3.12 Wireless Message Filtering

When configured as a Bridge, the XYR 400E will transmit all broadcast messages appearing at its wired Ethernet port. When the XYR 400E is configured as a Router, this does not occur.

In many cases, the intended recipient of the broadcast traffic does not lie at the opposite end of a proposed radio link. Reducing unnecessary broadcast traffic sent over the radio link, will increase available bandwidth for data. The XYR 400E has a filtering feature to help reduce unnecessary wireless transmissions and enhance security.

The XYR 400E may be configured to reject or accept messages to and from certain Addresses. To accept wireless messages from particular devices a "Whitelist" of Addresses must be made. Alternatively to reject messages from particular devices, a "Blacklist" of Addresses must be made. Filtering applies only to messages appearing at the wired Ethernet port of the configured XYR 400E.

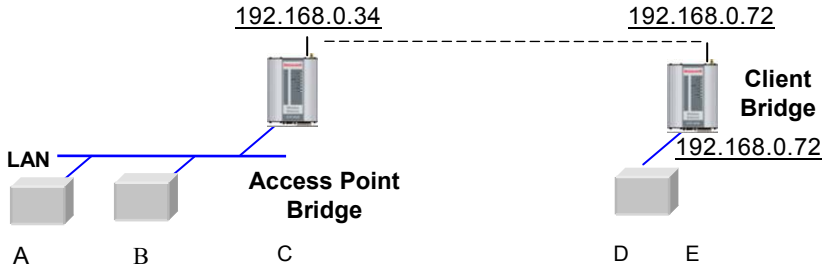
The Filter comprises of two lists: one of MAC Addresses and another listing IP protocol details. Each list may be set as either a blacklist (to block traffic for listed devices and protocols), or as a whitelist (to allow traffic for listed devices and protocols). The Filter operates on two rules listed below.

1. A Blacklist has priority over a whitelist. Traffic matching detail in a blacklist will be discarded if it also appears in a whitelist.

2. When one or both lists are whitelists, traffic must have matching detail in at least one of the whitelists for it to be passed. Note that, as this must agree with rule 1 above, the traffic detail must not match anything in a blacklist, if present, for it to be passed.

When configuring a Whitelist it is important to add the Addresses of all devices connected to the XYR 400E wired Ethernet port, that communicate over the wireless link. It is particularly important to add the Address of the configuration PC to the Whitelist. Failure to add this address will prevent the configuration PC from making any further changes to configuration. Design of the filter may be simplified by monitoring network traffic and forming a profile of traffic on the wired network. Network Analysis software, such as the freely available Ethereal program, will list broadcast traffic sent on the network.

For example, Computer B sees the computer D via Ethernet Modems C & E. The White Filtering requires that at Modem C has computer B in its white list, Modem E has computer D in its Whitelist. Computer A will be not be able to access Computer D, as Computer A is not present in the Whitelist in Modem C.



If radio links are chained together to form a radio backbone, it is also important to consider the operation of the Layer 3 Transparent Bridge (Refer Section 3.7). A XYR 400E Client will act as a MAC Address translator, as it acts as a MAC address proxy on behalf of devices connected to its wired Ethernet port. Addition of XYR 400E Client MAC addresses into intermediate XYR 400E units' whitelist filters may be required for correct operation.

It is advisable to use the Apply Changes button to test the configuration entered. Once the configuration is determined to be correct, the Apply Changes and Save button should be used. In the event that the configuration is incorrect, a power reset will revert the unit to previously saved configuration.

If an erroneous configuration has prevented all access to the module, SETUP mode may be used analyze what is wrong with the configuration. Simply switch the dipswitch to SETUP and cycle power. The XYR 400E will retain its configuration, however will load up at IP address 192.168.0.1XX, netmask 255.255.255.0 with the radio and filter disabled. The *XX in the IP address* is the last two digits of the serial number. Configuration webpages will still show the original configuration. No changes are made to configuration until the user saves changes. To resume normal operation, set the dipswitch to RUN and cycle power.

MAC Address Filter Configuration:

Add Entries	Enter the MAC addresses of devices to be added to the list. Multiple entries must be separated by a semi-colon (;).
Delete Entries	Check the box alongside entries selected for removal from the list.
Whitelist or Blacklist	Check the box to make the list a whitelist. This will allow devices with the MAC addresses listed to communicate with the module and utilize the radio link. All other devices are blocked unless they exist in an IP whitelist. Uncheck the box to make the list a blacklist. This will prevent all listed devices from using accessing the module and using the radio link.
Apply Changes	Update settings.
Apply Changes and Save	Update settings and save to non-volatile memory.

IP Address Filter Configuration:

Add Entries	Enter the details of IP traffic to be added to the list. Protocols ARP, ICMP, TCP and UDP may be selected. Other IP protocols may be selected provided the IP protocol number within packets is known. TCP and UDP traffic may be also limited to specific port numbers.
Delete Entries	Check the delete box alongside entries selected for removal from the list. Alternatively, check the enable box alongside entries if you want to make the rule active.
Whitelist or Blacklist	Check the box to make the list a whitelist. This will only allow traffic described in the list to be sent over the radio link. All other traffic is blocked unless it is present in a MAC whitelist. Uncheck the box to make the list a blacklist. This will ban all traffic described in the list from being sent to the module or over the radio link.
Apply Changes	Update settings.
Apply Changes and Save	Update settings and save to non-volatile memory.

NOTE: When configuring a TCP filter it is often desirable to also configure both an ARP and an ICMP filter for the same IP Address range. The ARP filter is required whenever the sending device does not have a fixed IP to MAC Address translation table entry (i.e. whenever the device may need to send an ARP request to determine the MAC address of a device with a known IP Address). An ICMP filter is needed to allow/disallow “pings”.

3.13 Serial Port Configuration

The XYR 400E has an RS-232, and RS-485 port for serial communications. These ports may be used for different purposes. The XYR 400E offers three different serial functions which are PPP server, Serial Gateway, and Modbus TCP to RTU Gateway.

3.13.1 RS-232 PPP Server

The XYR 400E can be used as a PPP Server to connect the wireless Ethernet system to serial devices via the RS232 or RS485 serial ports.

PPP Server enables a network connection to the XYR 400E over a serial cable. This is much like dial up internet. The maximum serial data rate is 115,200bps. Hardware or Software flow control may be selected.

With minimal configuration on the PC, you may use Dial up networking in Windows XP to connect to the network via the serial port.

For the XYR 400E, users must configure the local IP address for the XYR 400E and the remote device IP address. Some care must be taken in selecting these IP addresses.

If you wish to use routing over this serial network connection, then the IP addresses selected must not lie on Wireless or Wired Ethernet networks already configured into the device. You must ensure they set routing rules appropriately for devices either side of the network.

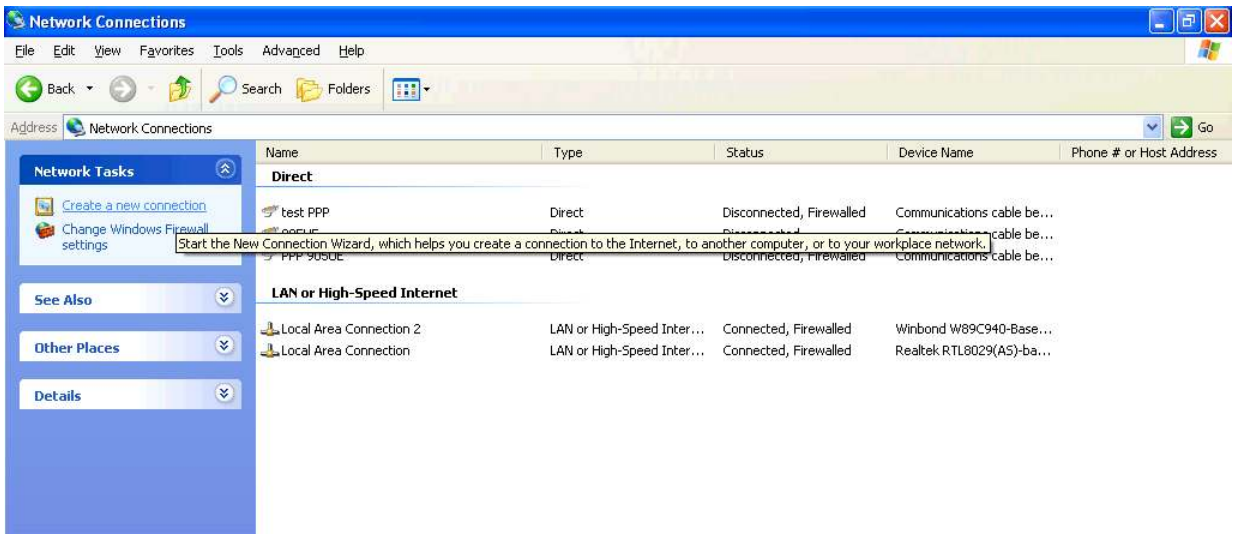
If you want the serial device visible as present on the Wireless or Wired network, then the local IP address must be the same as the IP address set for the desired port. A process called "Proxy ARP" is used to make the device visible on the network. In this process, the XYR 400E pretends that it holds the IP address on the network, and responds on behalf of the remote device.

The result of this is similar to bridging for a single device, with some exceptions. One of these exceptions is the inability to handle name server searches of the network via this serial link. For example, you would encounter difficulty if you were to use Windows Explorer over the serial link to find a PC on the wired network. For this to operate correctly you must explicitly map computer names to IP addresses in the "LMHOSTS" file on your PC.

When in SETUP mode, the XYR 400E PPP server is enabled. This may also be used to configure the module. Settings whilst in SETUP mode are as follows:

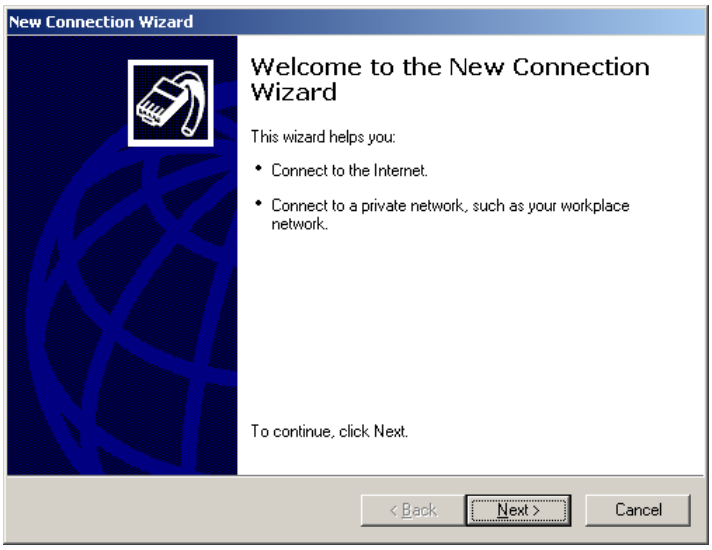
- username *user*, password is *user*.
- Serial baud rate 38400bps
- Hardware flow control
- Local address 192.168.123.123
- Remote address 192.168.123.124

To configure Windows XP to establish a PPP connection to a XYR 400E in SETUP mode, follow these steps:

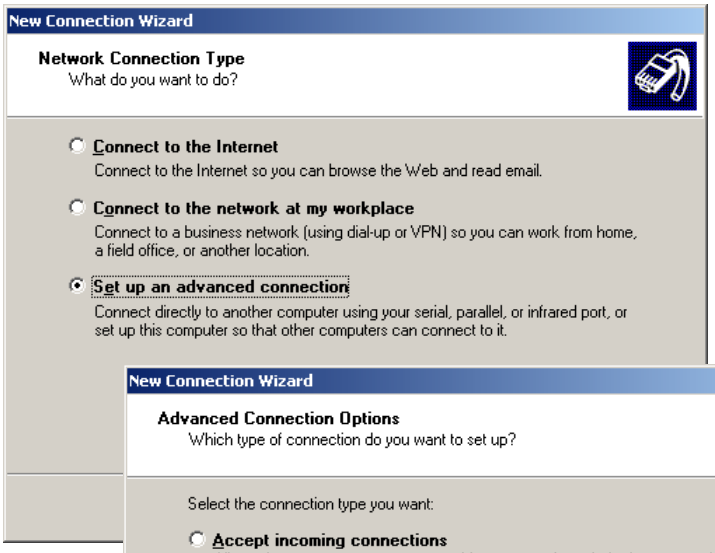

Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Network Tasks
Create a new connection
Change Windows Firewall settings
See Also
Other Places
Details
Name Type Status Device Name Phone # or Host Address
Direct
test PPP Direct Disconnected, Firewalled Communications cable be...
Start the New Connection Wizard, which helps you create a connection to the Internet, to another computer, or to your workplace network.
LAN or High-Speed Internet
Local Area Connection 2 LAN or High-Speed Inter... Connected, Firewalled Winbond W89C940-Base...
Local Area Connection LAN or High-Speed Inter... Connected, Firewalled Realtek RTL8029(AS)-ba...

1. On Network Connections in Windows XP, select Create a new connection

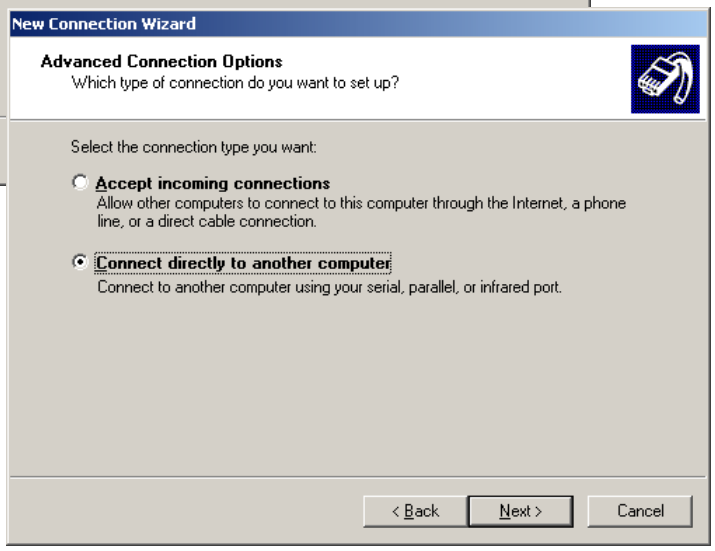
2. On the New Connection Wizard, click Next


New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
• Connect to the Internet.
• Connect to a private network, such as your workplace network.
To continue, click Next.
< Back
Next >
Cancel

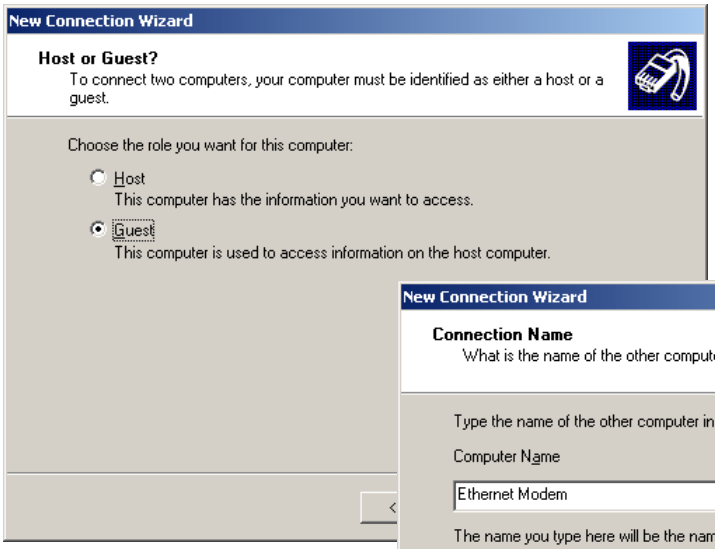
3. Set up an advanced connection


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

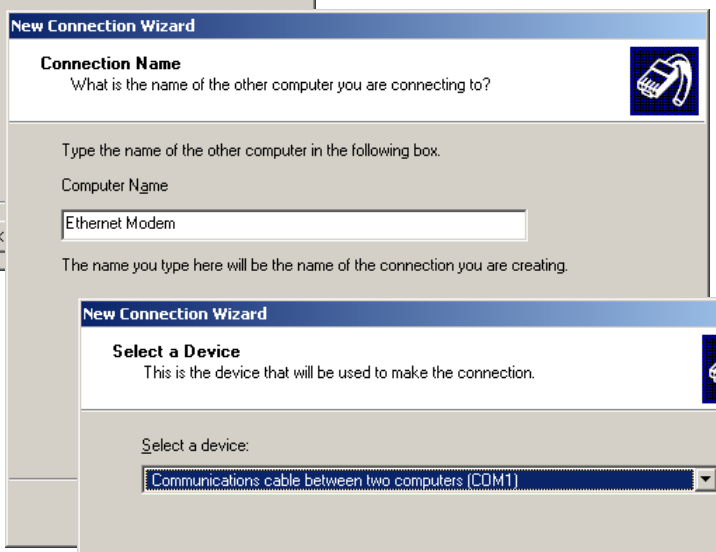
4. Connect directly to another computer


New Connection Wizard
Advanced Connection Options
Which type of connection do you want to set up?
Select the connection type you want:
Accept incoming connections
Allow other computers to connect to this computer through the Internet, a phone line, or a direct cable connection.
Connect directly to another computer
Connect to another computer using your serial, parallel, or infrared port.
< Back
Next >
Cancel

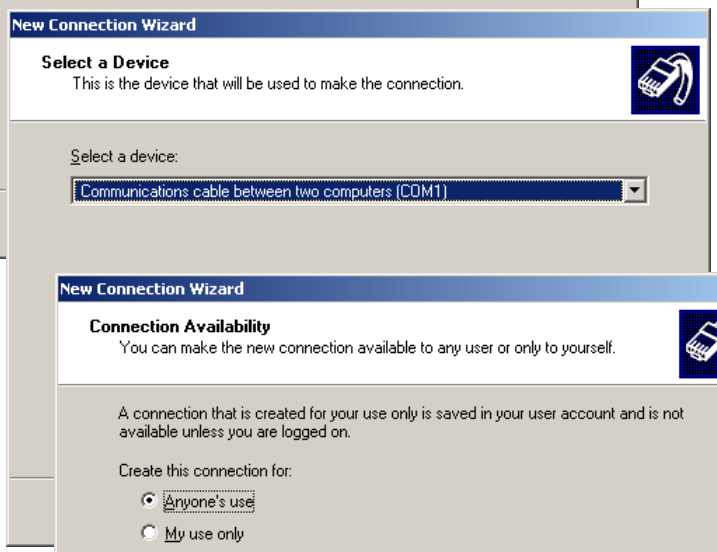
5. Set PC as guest


New Connection Wizard
Host or Guest?
To connect two computers, your computer must be identified as either a host or a guest.
Choose the role you want for this computer:
Host
This computer has the information you want to access.
Guest
This computer is used to access information on the host computer.

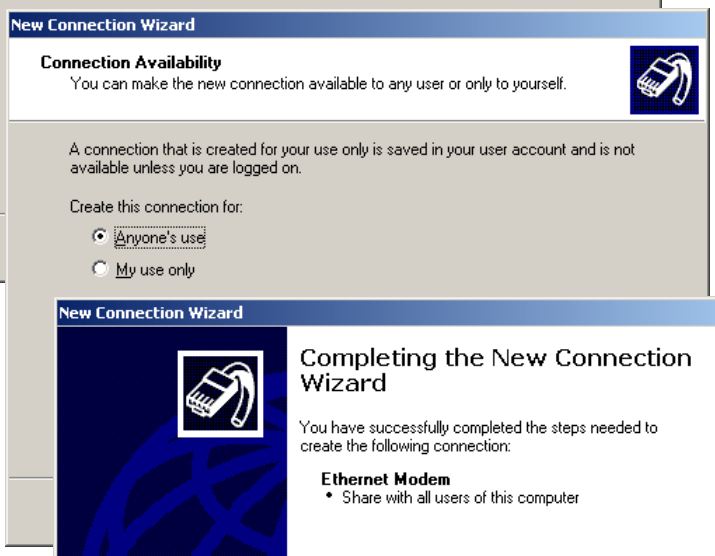
6. Set Computer Name


New Connection Wizard
Connection Name
What is the name of the other computer you are connecting to?
Type the name of the other computer in the following box.
Computer Name
Ethernet Modem
The name you type here will be the name of the connection you are creating.

7. Select a COM port


New Connection Wizard
Select a Device
This is the device that will be used to make the connection.
Select a device:
Communications cable between two computers (COM1)

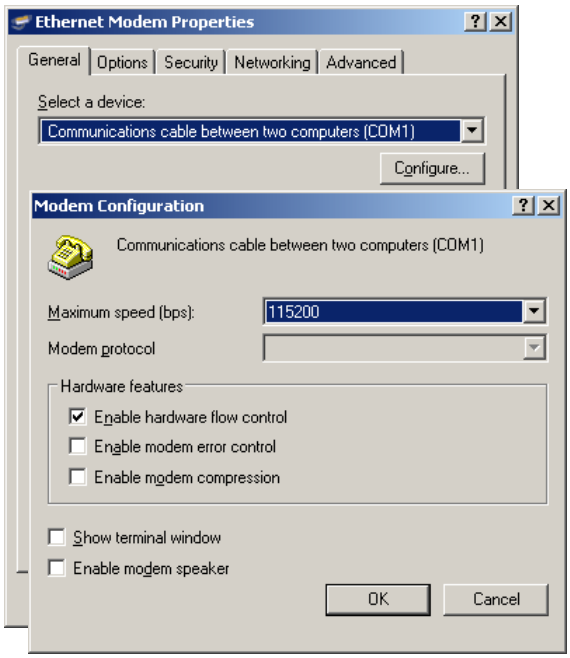
8. Select availability


New Connection Wizard
Connection Availability
You can make the new connection available to any user or only to yourself.
A connection that is created for your use only is saved in your user account and is not available unless you are logged on.
Create this connection for:
Anyone's use
My use only

9. Click Finish

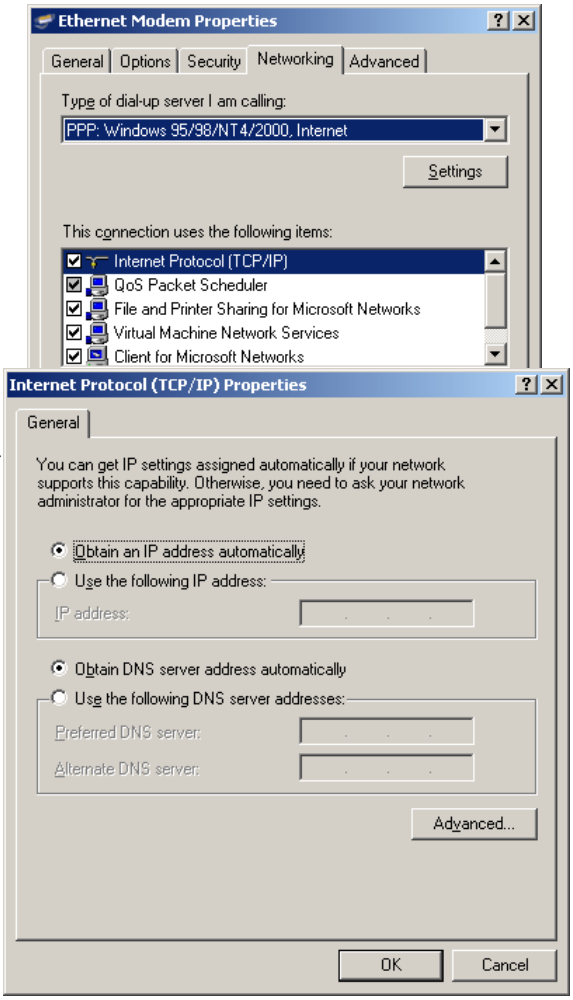
New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
Ethernet Modem
• Share with all users of this computer
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel

10. Select properties of this new connection by right clicking on connection.



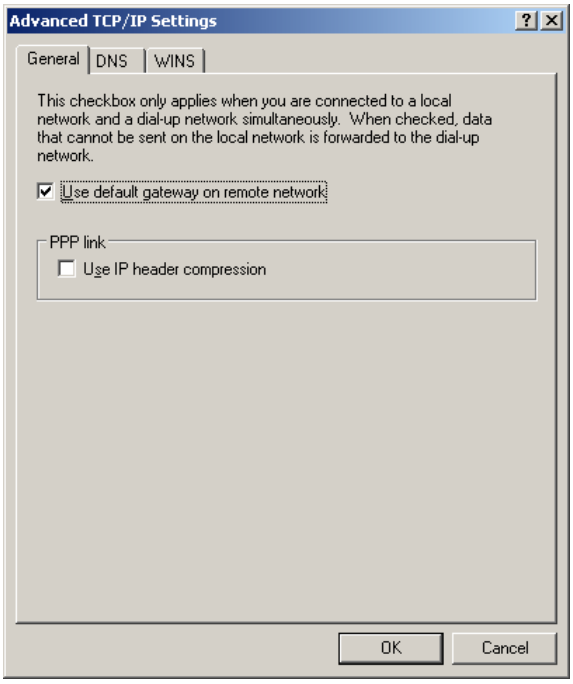
11. General Tab click on Configure button

12. Ensure maximum speed is 115200bps, click OK



13. Select Networking Tab -> click on Internet Protocol (TCP/IP) in list box and then click Properties button.

14. On Properties form click Advanced button


Advanced TCP/IP Settings
General
DNS
WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network
PPP link
Use IP header compression
OK
Cancel

15. On Advanced TCP/IP Settings form->General Tab, uncheck field in PPP link stating "Use IP header compression".

16. Configuration is now complete. Click on this newly created link to establish a connection to XYR 400E.

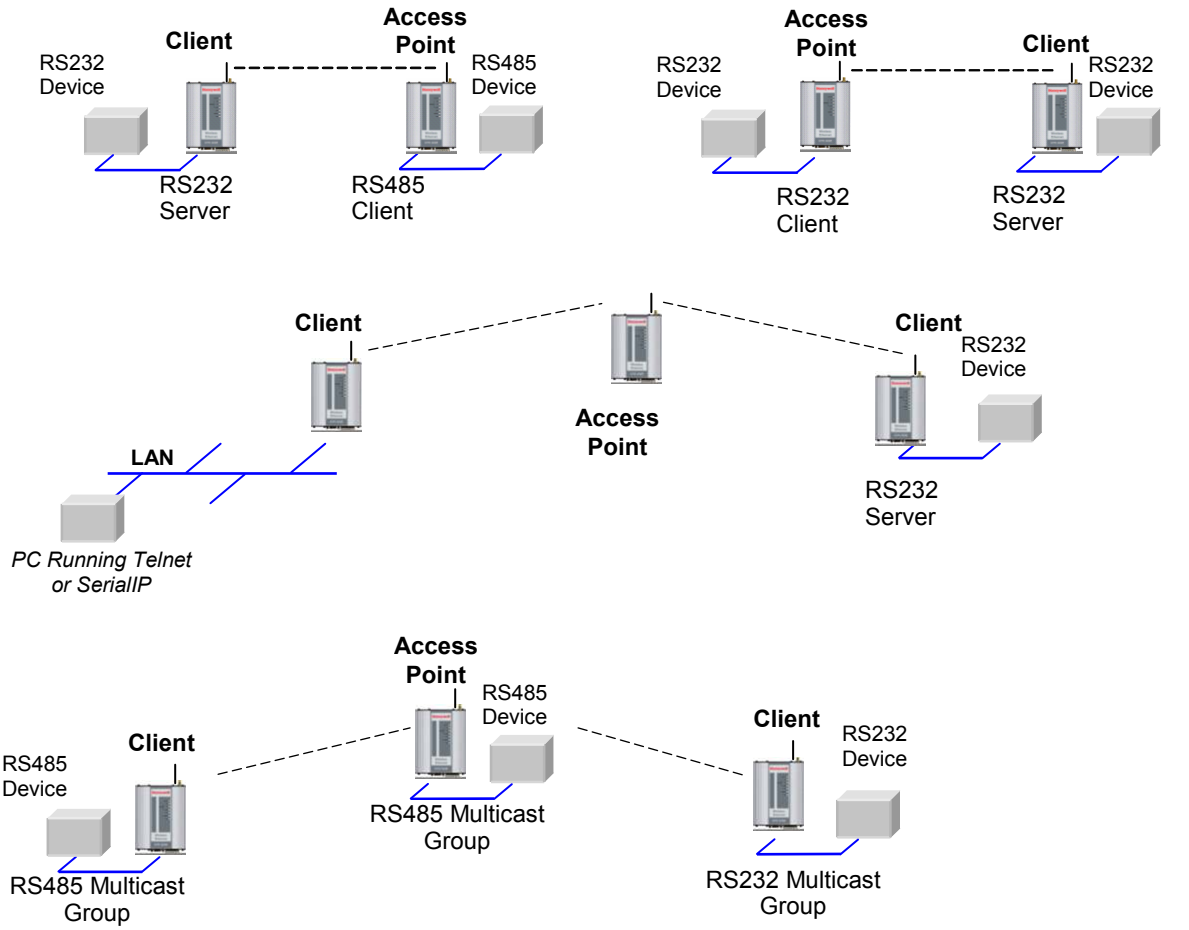
17. Ensure both the username and the password are entered exactly as configured in XYR 400E. (When booted in SETUP mode, the PPP server has username “user” and password “user”.)

3.13.2 Serial Gateway

Serial Gateway functionality is available for both RS-232 and RS-485 ports independently, and enables serial data to be routed via the wired or wireless network connection. Serial Gateway functionality is similar to radio modem functionality, allowing point-to-point and multipoint serial data transfer.

Each XYR 400E serial port may be configured as Server, Client, or Multicast Group. When configured as Server, the module will wait for a connection to be initiated by a remote client. When configured as Client, the module will automatically attempt to connect to the specified remote server. When configured as Multicast Group, the module will broadcast data to all members of the same Multicast Group.

Some of the possible Serial Gateway topologies are illustrated below. As can be seen, it is possible for serial data from a XYR 400E to be transferred to one or more XYR 400E serial ports, or to be encapsulated within a TCP/IP socket for availability on an Ethernet network. Conversely, data encapsulated in a TCP/IP socket can be reproduced at a XYR 400E serial port. Both XYR 400E serial ports and the hard wired Ethernet port can be in use at the same time.



There are software packages available (i.e. SerialIP Redirector by Tactical Software) that can create a virtual serial port on a PC. This virtual serial port can be configured to connect to a XYR 400E serial port. Standard programs can then be used to access this serial port as if it were actually

connected to the PC. Alternatively the program telnet may be used to connect to a serial port on the XYR 400E. The telnet command used should be:

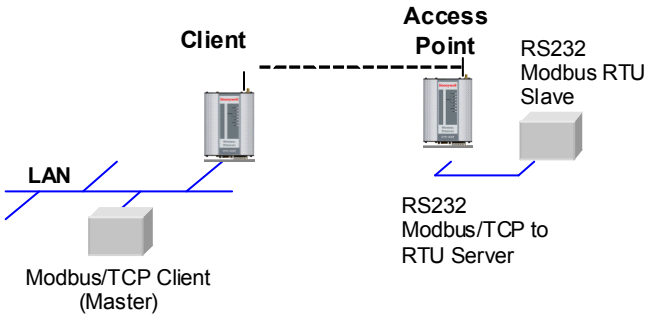
TELNET *[IP address] [Listen Port]*

eg. TELNET 192.168.0.155 23 where the *IP address* is 192.168.0.155 and *Listen Port* is 23.

Enable RS-232 PPP Server	Check this box to enable the PPP network server on the RS-232 port.
Enable RS-485 Serial Gateway	Check this box to enable the Serial Gateway Server on the RS-485 port.
Data Rate	The serial data rate desired. Serial data rates available range from 110bps to a maximum of 115,200bps.
Data Bits Parity Stop Bits	The data format desired. Data formats of 8N1, 7E1, 7O1, 7E2, 7O2 are supported.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Server	When configured as Server, the module will wait for a connection to be initiated by a remote client
Listen Port	Server Only. Enter the TCP port number on which the server must listen for incoming connections. The standard TELNET port is 23.
Client	When configured as Client, the module will automatically attempt to connect to the specified remote server
Remote Device Port	Client only. Enter the TCP port number of the remote server (i.e. the remote port to automatically connect to).
Remote Device IP Address	Client only. Enter the IP Address of the remote server (i.e. the remote IP Address to automatically connect to).
Multicast Group Port	Enter the UDP port number that all members of the group will use (i.e. all group members should use the same port number).
Multicast Group IP	Enter a valid Multicast IP Address identifying the group (i.e. all group members should use the same Multicast Group IP Address). Valid Multicast IP Addresses are in the range 224.0.1.0 to 238.255.255.255.

3.13.3 Modbus TCP to RTU Gateway

The Modbus TCP to RTU Gateway allows an Ethernet Modbus/TCP Client (Master) to communicate with a serial Modbus RTU Slave. The XYR 400E makes this possible by internally performing the necessary protocol conversion. The conversion is always performed by the XYR 400E which is directly connected to the Modbus serial device (i.e. only this module needs to have Modbus TCP to RTU Gateway enabled).



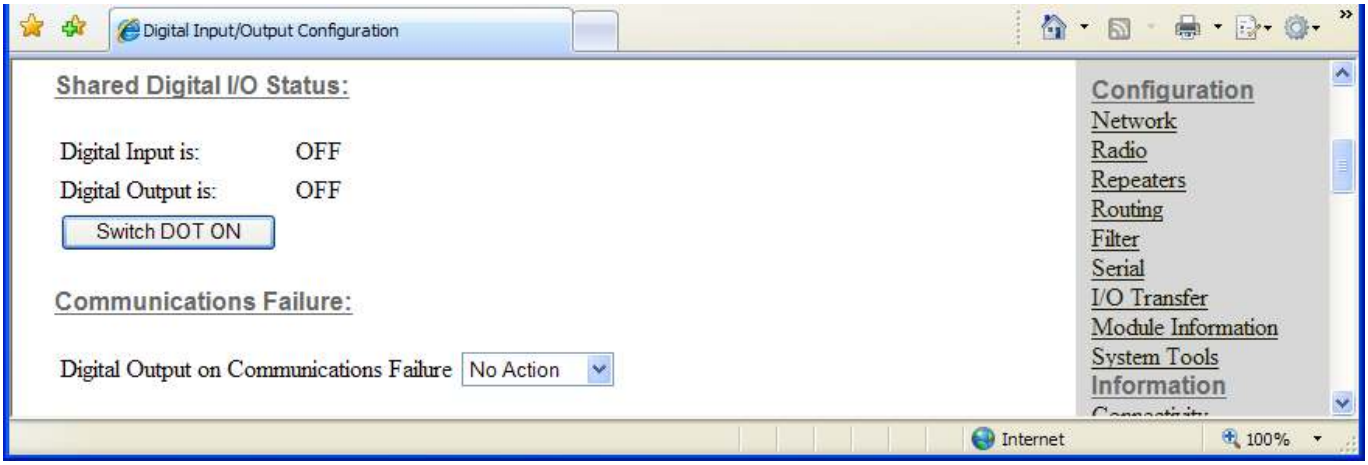
The above example demonstrates how a Modbus/TCP Client (Master) can connect to one or more Modbus RTU (i.e serial) Slaves. In this example the XYR 400E Access Point is configured with the "RS232 Modbus/TCP to RTU Gateway" enabled. Once enabled, the gateway converts the Modbus/TCP queries received from the Master into Modbus RTU queries and forwards these over the RS232 port to the Slave. When the serial response to the query arrives from the Slave, it is converted to a Modbus/TCP response and forwarded via the network to the Modbus/TCP Master. If no response was received serially by the XYR 400E within the configured Response Timeout, the XYR 400E will initiate a number of retries specified by the configured Maximum Request Retries.

The Modbus TCP to RTU Gateway may be configured to operate on either the RS-232 or RS-485 port. It does not support operation on both ports at the same time.

Enable RS-232 Modbus TCP to RTU Gateway	Check this box to enable the Modbus TCP to RTU Gateway on the RS-232 port. Only a single serial port is allowed at a time.
Enable RS-485 Modbus TCP to RTU Gateway	Check this box to enable the Modbus TCP to RTU Gateway on the RS-485 port. Only a single serial port is allowed at a time.
Data Rate	The serial data rate desired. Serial data rates available range from 110bps to a maximum of 115,200bps.
Data Bits Parity Stop Bits	The data format desired. Data formats of 8N1, 7E1, 7O1, 7E2, 7O2 are supported.
Pause Between Requests	Enter the delay between serial request retries in milliseconds
Response Timeout	Enter the serial response timeout in milliseconds – a serial retry will be sent if a response is not received within this timeout.
Connection Timeout	Enter the TCP connection timeout in seconds – if no Modbus/TCP data is received within this timeout then the TCP connection will be dropped. Set this field to zero for no timeout.
Maximum Request Retries	Enter the maximum number of request retries performed serially.
Maximum Connections	Enter the maximum number of simultaneous TCP connections to the server allowed.

3.14 Digital Input/Output

The functionality of the shared Digital Input/Output pin may be configured via the "I/O Transfer" internal webpage. As this pin is shared, the Digital Input status will be ON when the Digital Output is set ON.



The Digital I/O channel can be transferred to/from another device using Modbus (see section "3.15 Modbus I/O Transfer" below) or it can be configured to provide status of the module communications. If the XYR 400E disassociates from another unit (that is, there is no wireless link), you can configure the digital output to turn ON (set) or OFF (drop).

3.15 Modbus I/O Transfer

The XYR 400E provides Modbus TCP Client and Modbus TCP Server functionality for I/O transfer. 5000 x 16bit general purpose registers are provided for Modbus (including the onboard Digital Input/Output) and are shared for both Client and Server. Modbus TCP Client (Master) and Modbus TCP Server (Slave) are both supported simultaneously, and when combined with the built in Modbus TCP to RTU Gateway the XYR 400E can transfer I/O to/from almost any combination of Modbus TCP or RTU devices.

The layout of the XYR 400E I/O Registers is summarized in the table below. Each register is internally saved as a 16 bit value. A Modbus transaction may access the entire 16 bit value of any register, or alternatively the most significant bit of a register may be accessed as a discrete value. The main use for the general purpose I/O registers is for intermediate storage, i.e. when transferring I/O from one Modbus Slave device to another. Also provided is the status of the onboard digital I/O, as well as the status of the wireless link. The 16 bit status register contains the value FFFF(hex) for ON and 0000(hex) for OFF. Inverted status registers are also provided where the registers contain 0000(hex) for ON and FFFF(hex) for OFF.

Registers	Purpose
1 – 4299	General purpose I/O registers (read/write)
4300	On-board Digital Input value (read only)
4301	Link Status (read only)
4320	On-board Digital Output value (read/write)
4370	On-board Digital Input inverted value (read only)
4371	Link Status inverted (read only)
4372-4999	Reserved for future use

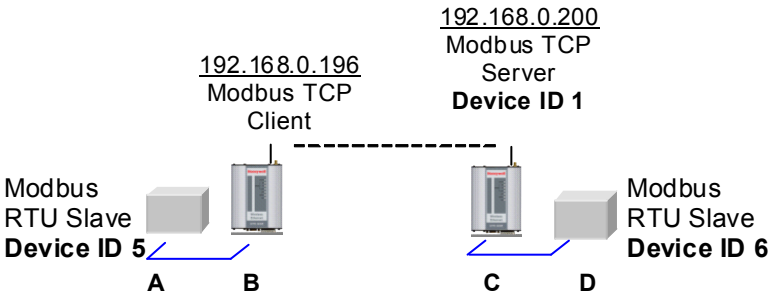
Modbus TCP Client (Master) enables the XYR 400E to connect to one or more Modbus TCP Servers (Slaves). All Modbus Master messages are directed either to/from the onboard I/O registers depending on configuration (described below). The Modbus TCP Client may also poll Modbus RTU (i.e. serial) devices connected to either the local serial port or a remote XYR 400E serial port by enabling the Modbus TCP to RTU gateway at the corresponding serial port (see section "3.13.3 Modbus TCP to RTU Gateway"). Modbus TCP Client functionality allows connections to a maximum of 25 different Modbus TCP Servers.

Modbus TCP Server (Slave) enables the XYR 400E to accept connections from one or more Modbus TCP Clients (Masters). All Modbus transactions routed to the onboard Modbus TCP Server are directed either to/from the onboard general purpose I/O registers. The Modbus TCP Server is shared with the Modbus TCP to RTU Gateway, so that the Modbus "Device ID" is used to determine if a Modbus transaction is to be routed to the onboard Modbus TCP Server or to a Modbus RTU device connected to the serial port. Care should therefore be taken that all serially connected Modbus devices use a different Modbus Device ID (i.e. Modbus Slave Address) to the onboard Modbus TCP Server. Up to 32 separate connections to the Modbus TCP Server are supported.

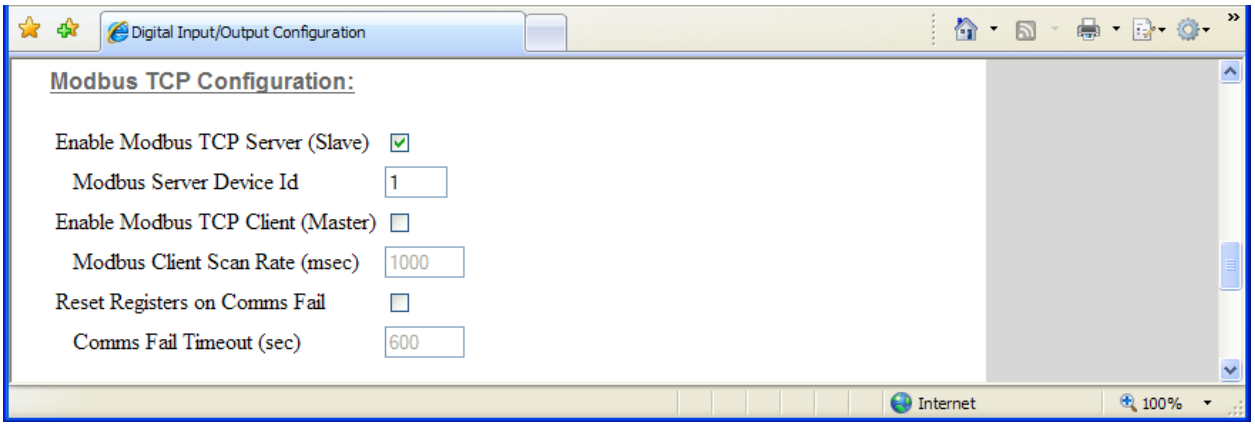
Modbus RTU (serial) Master functionality is achieved by combining the Modbus TCP Client (Master) and Modbus TCP to RTU Gateway. Simply specify a Modbus TCP Client (Master) connection to a Modbus TCP Server where the server is the address of any XYR 400E with Modbus TCP to RTU Gateway enabled. Care should be taken to ensure that the Device ID (i.e. Modbus Address) of the serial device is different to the Device ID of the onboard Modbus TCP Server of the XYR 400E that the serial device is connected to.

The XYR 400E provides a configurable option to automatically reset the value of the onboard I/O registers to zero in the event of a communications failure. If a valid Modbus transaction directed to/from a given register has not been completed for longer than a configurable timeout, then the value of that register will be reset to zero.

An example of the Modbus functionality of the XYR 400E is illustrated below. In this example the status of the onboard digital input at C will be reflected at the onboard digital output at B. Also, 8 I/O registers from Modbus serial device D will be transferred to A.



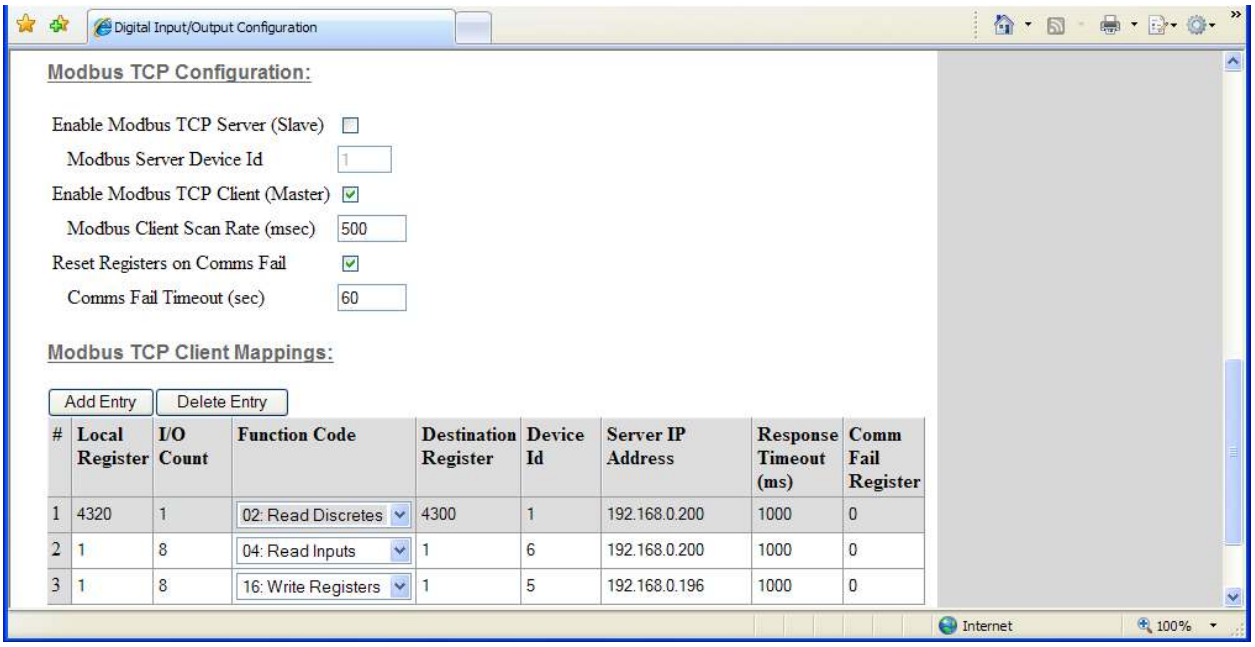
The Modbus configuration for unit C is shown below. Unit C is configured with Modbus TCP Server enabled and Device ID = 1, so that the Modbus TCP Client at B can connect and read the status of the onboard digital input. Unit C also has Modbus TCP to RTU Gateway enabled (see section "3.13.3 Modbus TCP to RTU Gateway") so that the Modbus TCP Client at B can communicate with the serial Modbus RTU device D.



The configuration of unit B is shown below (accessible via the "I/O Transfer" configuration page). It can be seen that Modbus TCP Client has been enabled with a 500msec scan rate, meaning that there will be a 500msec delay between each of the *mappings* directed at any server. The "Reset Registers on Comms Fail" option is enabled with a timeout of 60 seconds, indicating that any of the registers at unit B will be reset if a successful Modbus transaction involving that register has not been executed in the last 60 seconds. The Modbus TCP to RTU Gateway at B must also be enabled (see section "3.13.3 Modbus TCP to RTU Gateway") to allow Modbus communications with the serial device A.

Three "Modbus TCP Client Mappings" are also configured at B in order to perform the required I/O transfer. The first mapping transfers the status of the onboard digital input at C to the onboard digital output at B. *Local Register* 4320 specifies the register for the onboard digital output at B (since B is the *local* unit at which the mapping is configured). *I/O Count* 1 specifies that only one I/O point is being transferred (i.e. the single digital I/O). *Function Code* 02: Read Discretes specifies the standard Modbus function code to read discrete (i.e. digital) inputs. *Destination Register* 4300 specifies the register for the onboard digital input at unit C (since C is the *destination* unit for this mapping). *Device ID* 1is the ID of the onboard Modbus TCP Server at C. *Server IP Address*

192.168.0.200 is the IP address of unit C – which is the Modbus TCP Server we are reading from. *Response Timeout* 1000 ms specifies that unit C must respond to this message within 1000ms. *Comm Fail Register* 0 specifies the local register where the communications status for this mapping will be stored.


Digital Input/Output Configuration
Modbus TCP Configuration:
Enable Modbus TCP Server (Slave)
Modbus Server Device Id
1
Enable Modbus TCP Client (Master)
Modbus Client Scan Rate (msec)
500
Reset Registers on Comms Fail
Comms Fail Timeout (sec)
60
Modbus TCP Client Mappings:
Add Entry
Delete Entry
| Local Register | I/O Count | Function Code | Destination Register | Device Id | Server IP Address | Response Timeout (ms) | Comm Fail Register
1 | 4320 | 1 | 02: Read Discretes | 4300 | 1 | 192.168.0.200 | 1000 | 0
2 | 1 | 8 | 04: Read Inputs | 1 | 6 | 192.168.0.200 | 1000 | 0
3 | 1 | 8 | 16: Write Registers | 1 | 5 | 192.168.0.196 | 1000 | 0
Internet
100%

The second mapping reads 8 registers from serial unit D into onboard registers in unit B. Note that in this case the specified Device ID 6 is the Modbus Address of the serial device D, while the Server IP Address 192.168.0.200 is the IP Address of unit C since the Modbus TCP to RTU Gateway at unit C converts the Modbus TCP message to Modbus RTU and routes it out the serial port to unit D.

The third mapping takes the 8 registers read by the second mapping and writes them to the serial unit A. The specified Device ID 5 is the Modbus Address of the serial device A, and the Server IP Address 192.168.0.196 is the IP Address of the local unit B since the local Modbus TCP to RTU Gateway is to route the message out the serial port to unit A.

Since the XYR 400E supports Modbus TCP Client and Server simultaneously, the Modbus TCP Server for unit B above could also be enabled. This would allow one (or more) external Modbus TCP Clients anywhere on the extended wired or wireless network to connect to unit B and monitor the status of the I/O registers – including the I/O at units A, C, and D. This is a very powerful and flexible feature which could, for example, be exploited by a central monitoring facility or SCADA.

The configurable Modbus I/O transfer options are summarized in the tables below.

Modbus TCP Configuration:

Enable Modbus TCP Server (Slave)	Check this box to enable the onboard Modbus TCP Server. All Modbus TCP connections to the module IP Address and specified Modbus Server Device ID will be routed to the onboard I/O registers.
Modbus Server Device ID	Specify the Modbus Device ID for the onboard Modbus TCP Server. Allowed values are 0 to 255.
Enable Modbus TCP Client (Master)	Check this box to enable the onboard Modbus TCP Client. I/O to be transferred via the Modbus TCP client is specified with Modbus TCP Client Mappings.
Modbus Client Scan Rate	Enter the delay (in milliseconds) between execution of consecutive Modbus TCP Client Mappings to the same Server.
Reset Registers on Comm's Fail	When Enabled the value in any onboard I/O register will be reset to zero if a valid Modbus transaction directed to/from the given register has not been completed for longer than the Comms Fail Timeout.
Comms Fail Timeout	The period of time after which onboard I/O registers will be reset if a valid Modbus transaction directed at that register has not completed.

Modbus TCP Client Mappings:

Local Register	Enter the starting onboard I/O register number that the specified Modbus Master transaction will transfer I/O to/from.
I/O Count	Specify the number of consecutive I/O register to be transferred for the specified transaction.
Function Code	Specify the Modbus Function Code for the transaction.
Destination Register	Enter the starting I/O register number in the destination device that the specified Modbus Master transaction will transfer I/O to/from.
Device ID	Enter the Modbus Device ID of the destination Modbus device
Server IP Address	Specify the IP Address of the destination Modbus TCP Server for the specified transaction.
Response Timeout	Enter the timeout (in milliseconds) to wait for a response to the specified transaction.
Comm Fail Register	Enter the onboard I/O Register number to store the communication status of the specified transaction. The Specified register will be set to 0 if communications is successful, 0xFFFF if there is no connection to the specified server, or 0xFFxx where xx is the Modbus Exception Code

3.16 Module Information Configuration

Module Information Webpage Fields

This configuration page is primarily for information purposes. With the exception of the password, the information entered here is displayed on the root webpage of the XYR 400E.

Password Configuration password.	When changing the password on this screen, it will be sent unencrypted over any wired network. If encryption is enabled on the XYR 400E, any radio communications are encrypted, and therefore hidden from radio eavesdroppers. Caution must only be taken if there are potential eavesdroppers on the wired network.
Device Name	A text field if you wish to label the particular XYR 400E.
Owner	A text field for owner name.
Contact	A text field for owner phone number, email address etc.
Description	A text field used for a description of the purpose of the unit.
Location	A text field used to describe the location of the XYR 400E.

3.17 Remote Configuration

Because a module configuration is viewed and changed in a web format (which is an Ethernet application), you can view or change the configuration of a remote module via the wireless link, provided the remote module is already "linked" to the local XYR 400E.

To perform remote configuration, connect a PC to the local module, run Internet Explorer and enter the IP address of the remote unit - the configuration page of the remote module will be shown and changes can be made. If the remote module is configured as a Router, enter the wireless IP address of the router, not the Ethernet address.

Care must be taken if modifying the configuration of a module remotely. If the Radio Configuration is changed, some changes made may cause loss of the radio link, and therefore the network connection.

It is advisable to determine path of the links to the modules you wish to modify, and draw a tree diagram if necessary. Modify the modules at the "leaves" of your tree diagram. These will be the furthest away from your connection point in terms of the number of radio or Ethernet links.

In a simple system, this usually means modifying the Client modules first and the Access Point last.

Setting a XYR 400E to Factory Default Settings

Access configuration webpages of XYR 400E. Refer section *Accessing Configuration inside a module for the first time*, or *Modifying an existing configuration*.

1. Click on System Tools Menu Item
2. Enter username “user” and password “user”, when prompted for password.

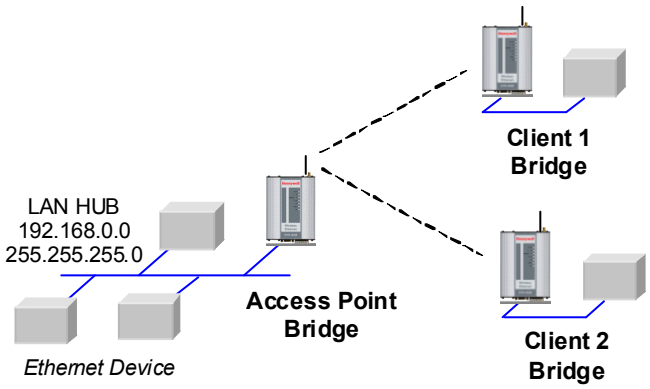
Click on Factory Default Configuration Reset, and wait for unit to reset. When reset, the LINK LED will flash.

Extending a wired network

Access Point Configuration

Connect straight through Ethernet cable between PC and XYR 400E.

- Ensure configuration PC and XYR 400E are setup to communicate on the same network
- Set dipswitch to SETUP mode.
- Power up unit, and wait for LINK led to cease flashing.



- Adjust PC network settings

  Set Configuration PC network card with network setting of IP address 192.168.0.1, netmask 255.255.255.0

- Open configuration webpage with Internet Explorer at address http://192.168.0.1XX/ where XX is the last two digits of the serial number

  When prompted for password, enter default username “user” and password “user”

  Enter “Network”, and select Operating Mode as Access Point.

  Select Device Mode as Bridge.

  Change the Gateway IP Address to 192.168.0.1

  Change the Ethernet and Wireless IP addresses to 192.168.0.200

  Change Ethernet and Wireless Subnet masks to 255.255.255.0

  Enter a System Address (SSID) string

  Select the Radio Encryption required.

Set dipswitch to RUN

Save the changes and unit will restart with new settings.

Alternate procedure – Adjust XYR 400E network settings using serial port(assuming configuration PC is on existing network)

a) Open terminal program with settings with data rate 19200bps, 8 data bits, 1 stop bit and no parity.

b) Set dipswitch to SETUP

c) Connect straight through serial cable to XYR 400E and power up unit.

d) When prompted, strike the Enter key to abort automatic boot

e) Set IP address of XYR 400E to 192.168.0.200 with command bip 192.168.0.200

f) Set netmask of XYR 400E to 192.168.0.200 with command bnm 255.255.255.0

g) Set gateway address of XYR 400E to 192.168.0.1 with command bgw 192.168.0.1

h) Set dipswitch to RUN

i) Reset XYR 400E with reset command.

j) Open configuration webpage with Internet Explorer at address http://192.168.0.200/

When prompted for password, enter default username "user" and password "user"

Enter "Network", and select Operating Mode as Access Point.

Select Device Mode as Bridge.

Change the IP address to 192.168.0.200

Enter a System Address (SSID) string

Select the Radio Encryption required, and enter the system keys. Make a record of these Encryption keys and use these on all modules in the system.

Set dipswitch to RUN

Save the changes and unit will restart with new settings.

Client 1 Configuration

Perform the same configuration steps as the Access Point configuration with the following differences:

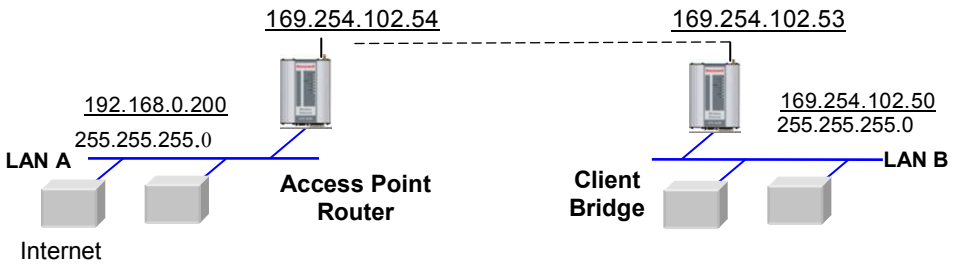
- set the Ethernet and Wireless IP addresses of XYR 400E to 192.168.0.201
- set the Operating Mode to Client.

Ensure the same System Generator String is used and the same Radio Encryption method is selected.

Client 2 Configuration

- As above, however set the Ethernet and Wireless IP addresses as 192.168.0.202

Connecting two separate networks together



Network A Configuration

In this example, network A is connected to the internet via a router at IP address 192.168.0.1.

Devices on Network A that only require access to devices on Networks A and B, should have their gateway IP address set to the XYR 400E Access Point as 192.168.0.200.

Devices on Network A, that must interact with devices on Networks A and B and the internet should set the internet router 192.168.0.1 as their gateway, and must have a routing rule established for devices on Network B. On PCs, this may be achieved with the MS-DOS command ROUTE. For this example use: ROUTE ADD 169.254.102.0 MASK 255.255.255.0 192.168.0.200

Network B Configuration

All devices on Network B should be configured so their gateway IP address is that of the XYR 400E Access Point as 169.254.102.54

Access Point Configuration

- Connect straight through Ethernet cable between PC and XYR 400E.
- Ensure configuration PC and XYR 400E are setup to communicate on the same network
- Set dipswitch to SETUP
- Power up unit, and wait for LINK led to cease flashing.
- Adjust PC network settings

  Set Configuration PC network card with network setting of IP address 192.168.0.1, netmask 255.255.255.0
- Open configuration webpage with Internet Explorer at address http://192.168.0.1XX/

  When prompted for password, enter default username “user” and password “user”

  Enter “Network”, and select Operating Mode as Access Point.

  Device Mode should be set to Router.

  Set the Gateway IP address to 192.168.0.1

  Set the Ethernet IP address to 192.168.0.200, network mask 255.255.255.0

  Set the Wireless IP address to 169.254.102.54, network mask 255.255.255.0

  Select the Radio Encryption required, and enter encryption keys if necessary.

Set dipswitch to RUN.

Click on button Save to Flash and Reset. Webpage will display that message indicating details are being written to flash. Wait for XYR 400E to reboot before removing power. Enter a System Generator String

Client Configuration

Perform the same configuration steps as the Access Point configuration with the following differences:

Enter "Network", and select Operating Mode as Client.

Device Mode should be set to Bridge.

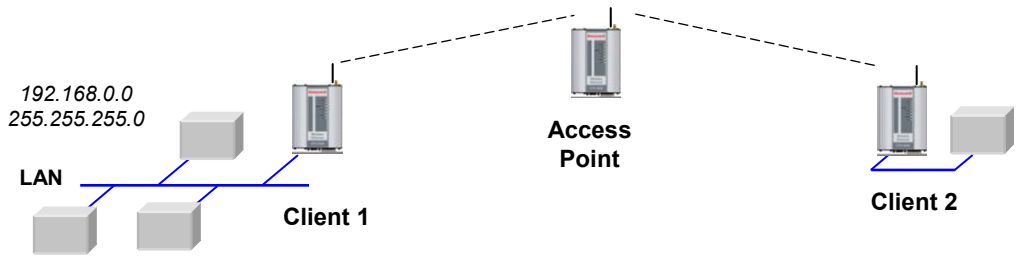
Set the Gateway IP address to 169.254.102.54

Set the Ethernet IP address to 169.254.102.53, network mask 255.255.255.0

Set the Wireless IP address to 169.254.102.53, network mask 255.255.255.0

Click on button Save to Flash and Reset. Webpage will display that message indicating details are being written to flash. Wait for XYR 400E to reboot before removing power.

Extending range of a network with a Repeater hop



Configure units as described in Section *Extending a wired network*. Place the Access Point at the remote intermediate repeater location. Additional repeaters can be added using Wireless Distribution System (WDS) – refer section 3.10 Repeater Configuration for further details.

Chapter Four DIAGNOSTICS

4.1 Diagnostics Chart

LED Indicator	Condition	Meaning
OK	GREEN	Normal Operation
OK	RED	Supply voltage too low.
Radio RX	GREEN flash	Radio receiving data
Radio TX	Flash	Radio Transmitting
Radio LINK	On	On when a radio communications link is established
Radio LINK	Off	Communications failure or radio link not established
LAN	ON	Link Established on Ethernet port
LAN	Flash	Activity on Ethernet port.
Serial	GREEN flash	Rs232 Serial Port Activity
Serial	RED flash	Rs485 Serial Port Activity
DIO	On	Digital Output ON ***or*** Input is grounded.
DIO	Off	Digital Output OFF ***and*** Input is open circuit.

The green OK LED on the front panel indicates correct operation of the unit. This LED turns red on failure as described above. When the OK LED turns red shutdown state is indicated. On processor failure, or on failure during startup diagnostics, the unit shuts down, and remains in shutdown until the fault is rectified.

Boot Loader LED Indication during Startup

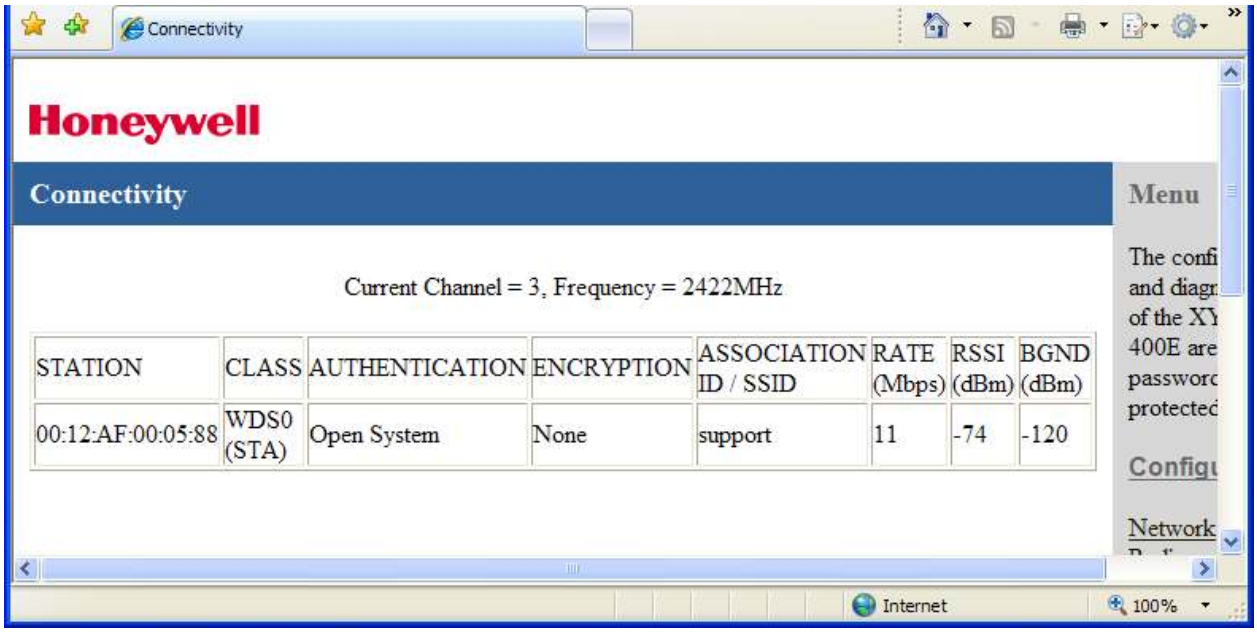
Serial	LAN	LINK	ACTIVE	Comment
Orange	Orange	Orange	RED	Initial Power Up & bootload Initialisation
RED	Orange	Orange	RED	Check Config & Print Sign-on message (If boot delay not zero)
Orange	Orange	Orange	RED	Print Configuration Table to terminal (If boot delay not zero)
Green	LAN	Off	RED	Initialise Networking and Start Auto Boot sequence
Orange	LAN	Off	GREEN	Wait for <ENTER> to abort Auto boot (If boot delay not zero)
Sequence	LAN	Sequence	GREEN	Boot – loader active (auto boot aborted or no application)
SERIAL	LAN	LINK	GREEN	Normal Operation. Application Running.

4.2 Diagnostic Information Available

4.2.1 Connectivity

The Connectivity webpage at an Access Point lists all Clients with which it is associated. The page also indicates whether the encryption scheme has been authorized at the Access Point. A XYR 400E will fail to be authorized if the encryption keys are incorrect.

The received signal strength, background noise, and radio data rate is listed for each Client or Access Point by their MAC Address. The readings shown are based upon the last received data message from the Access Point or Client. Generating radio traffic to the device will update values for signal strength, background noise and radio data rate. Use programs such as Ping to generate data packets to test the radio path.

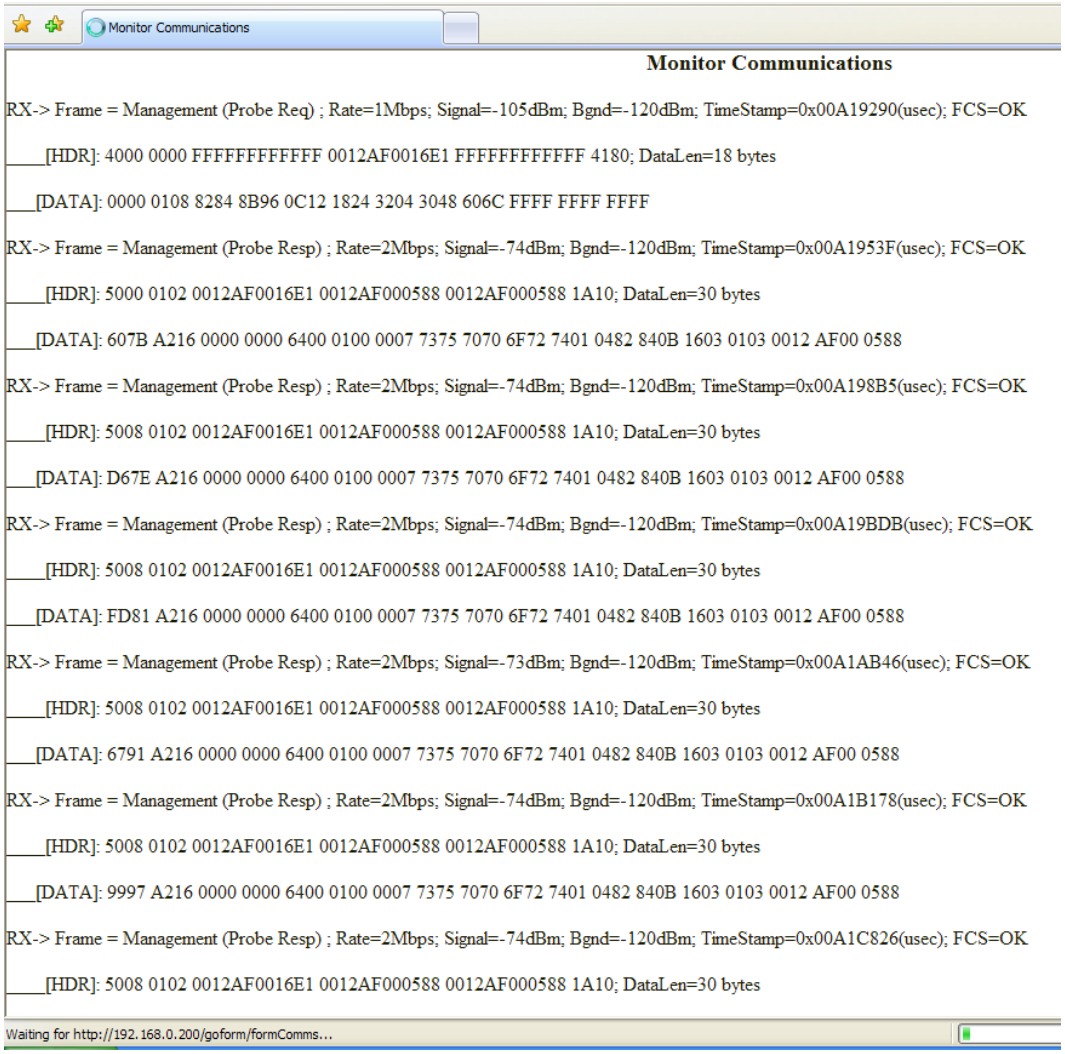


4.2.2 Monitor Communications

To monitor radio communications, it is necessary to configure the Operating Mode under "Network" as MONITOR. When in the MONITOR mode, the "Monitor Communications" function displays a continuous list of transmissions that are being received.

As Beacon messages occur very frequently, they have been filtered out from the Monitor Communications display for convenience.

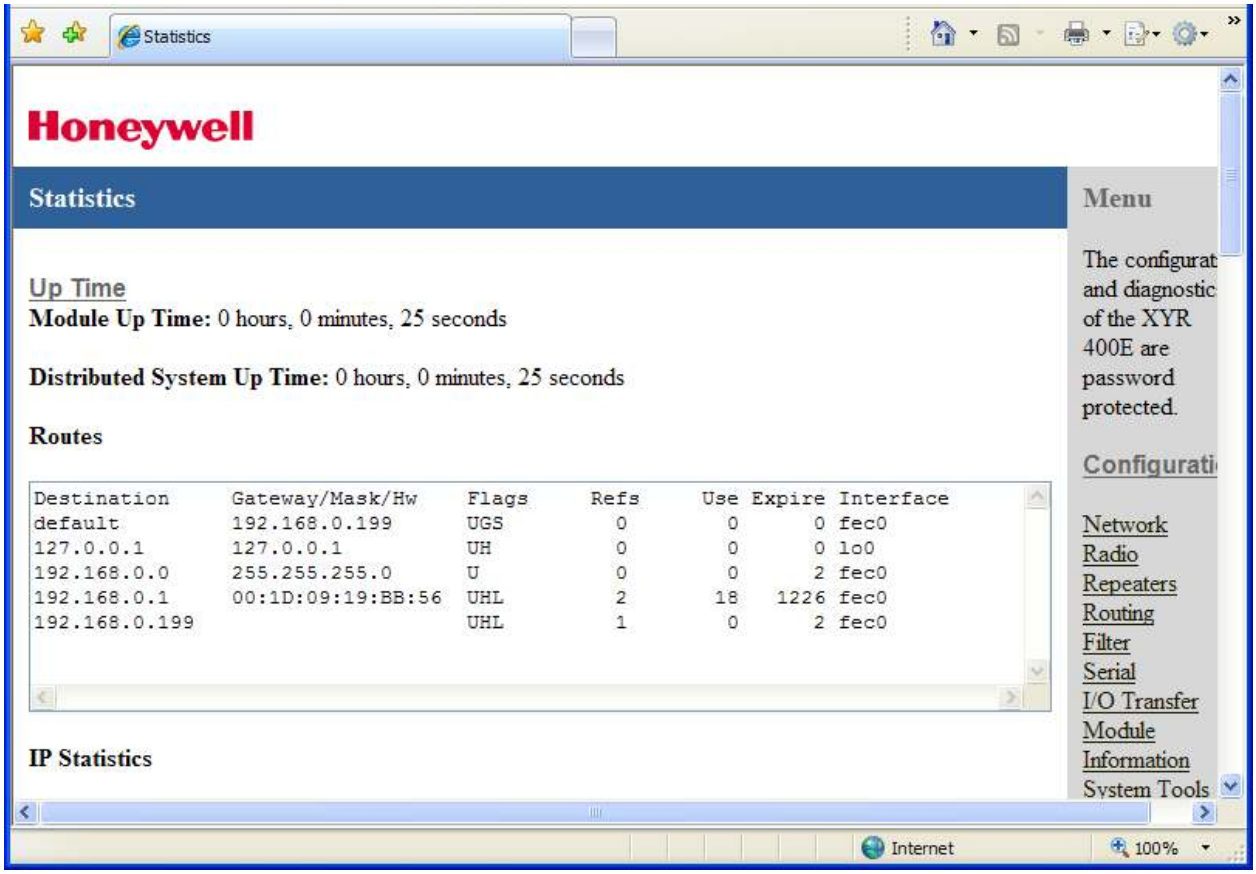
Monitor communications lists the frame type of each transmission and various statistics of each transmission, along with a timestamp. Communications can only be monitored on one channel at a time – the channel that is used for monitoring can be altered on the radio settings page.


Monitor Communications
Monitor Communications
RX-> Frame = Management (Probe Req) ; Rate=1Mbps; Signal=-105dBm; Bgnd=-120dBm; TimeStamp=0x00A19290(usec); FCS=OK
____[HDR]: 4000 0000 FFFFFFFFFFFF 0012AF0016E1 FFFFFFFFFFFF 4180; DataLen=18 bytes
___[DATA]: 0000 0108 8284 8B96 0C12 1824 3204 3048 606C FFFF FFFF FFFF
RX-> Frame = Management (Probe Resp) ; Rate=2Mbps; Signal=-74dBm; Bgnd=-120dBm; TimeStamp=0x00A1953F(usec); FCS=OK
____[HDR]: 5000 0102 0012AF0016E1 0012AF000588 0012AF000588 1A10; DataLen=30 bytes
___[DATA]: 607B A216 0000 0000 6400 0100 0007 7375 7070 6F72 7401 0482 840B 1603 0103 0012 AF00 0588
RX-> Frame = Management (Probe Resp) ; Rate=2Mbps; Signal=-74dBm; Bgnd=-120dBm; TimeStamp=0x00A198B5(usec); FCS=OK
____[HDR]: 5008 0102 0012AF0016E1 0012AF000588 0012AF000588 1A10; DataLen=30 bytes
___[DATA]: D67E A216 0000 0000 6400 0100 0007 7375 7070 6F72 7401 0482 840B 1603 0103 0012 AF00 0588
RX-> Frame = Management (Probe Resp) ; Rate=2Mbps; Signal=-74dBm; Bgnd=-120dBm; TimeStamp=0x00A19BDB(usec); FCS=OK
____[HDR]: 5008 0102 0012AF0016E1 0012AF000588 0012AF000588 1A10; DataLen=30 bytes
___[DATA]: FD81 A216 0000 0000 6400 0100 0007 7375 7070 6F72 7401 0482 840B 1603 0103 0012 AF00 0588
RX-> Frame = Management (Probe Resp) ; Rate=2Mbps; Signal=-73dBm; Bgnd=-120dBm; TimeStamp=0x00A1AB46(usec); FCS=OK
____[HDR]: 5008 0102 0012AF0016E1 0012AF000588 0012AF000588 1A10; DataLen=30 bytes
___[DATA]: 6791 A216 0000 0000 6400 0100 0007 7375 7070 6F72 7401 0482 840B 1603 0103 0012 AF00 0588
RX-> Frame = Management (Probe Resp) ; Rate=2Mbps; Signal=-74dBm; Bgnd=-120dBm; TimeStamp=0x00A1B178(usec); FCS=OK
____[HDR]: 5008 0102 0012AF0016E1 0012AF000588 0012AF000588 1A10; DataLen=30 bytes
___[DATA]: 9997 A216 0000 0000 6400 0100 0007 7375 7070 6F72 7401 0482 840B 1603 0103 0012 AF00 0588
RX-> Frame = Management (Probe Resp) ; Rate=2Mbps; Signal=-74dBm; Bgnd=-120dBm; TimeStamp=0x00A1C826(usec); FCS=OK
____[HDR]: 5008 0102 0012AF0016E1 0012AF000588 0012AF000588 1A10; DataLen=30 bytes
Waiting for http://192.168.0.200/goform/formComms...

Use of this feature together with the Connectivity webpage will reveal the variability of communications over a link, and other systems that may be in the area.

4.2.3 Statistics

The Statistics webpage is used for advanced debugging of XYR 400E. This webpage details the state of the XYR 400E and its performance in the system.



4.2.4 Network Traffic Analysis

There are many devices and PC programs that will analyse performance of an Ethernet network. Freely available programs such as Ethereal provide a simple cost effective means for more advanced analysis. By monitoring traffic on the wired Ethernet, a better idea of regular traffic can be discovered.

Network Analysis programs make configuration of a filter for the XYR 400E a simple task.

4.3 Testing Radio Paths

The general procedure for radio range testing a link is fairly simple. Configure two units to form a link using automatic radio rates. Install the Access Point at a fixed location. Take a laptop computer and the Client to each of the remote locations, and analyse the link using the Connectivity webpage. If a beacon is heard from the Access Point, the Client will update its Connectivity webpage with the received signal strength of beacon messages from the Access Point.

If the signal is strong enough, a link may be established, and the Connectivity webpage of the Access Point may be opened. If the link is weak, the LINK led will go out, and the remote Connectivity webpage of the Access Point will fail to load. Using this procedure, the signal strengths of units at both locations may be analysed, and traffic is sent between the units whilst remote WebPages are opened.

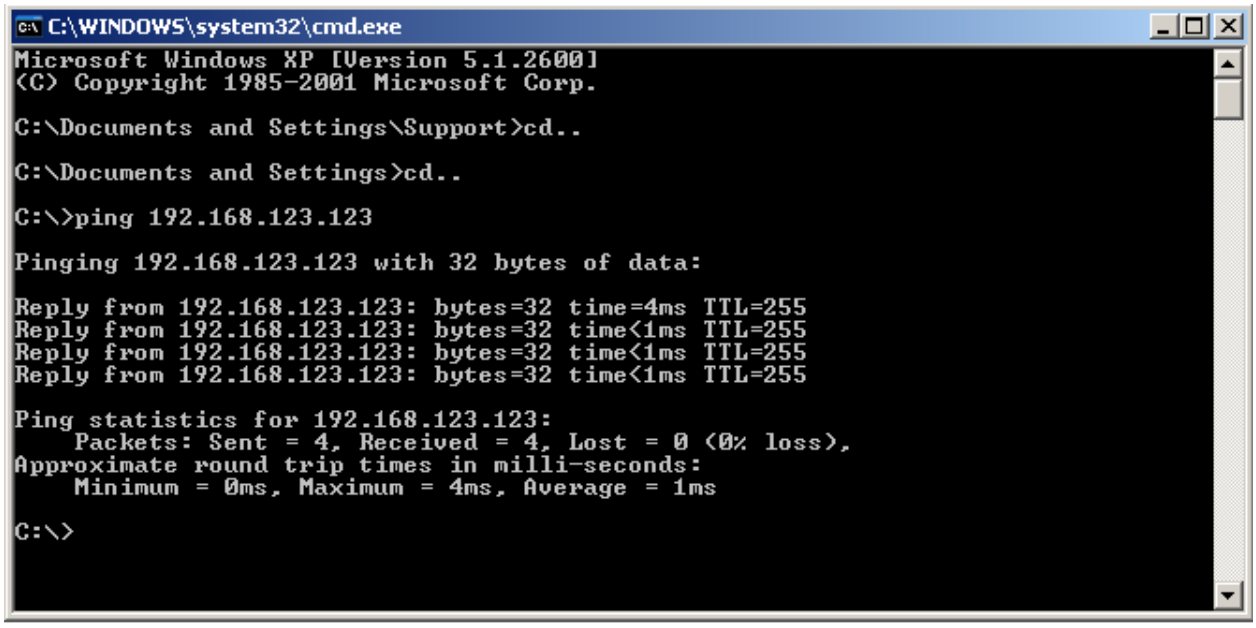
4.4 Utilities

4.4.1 PING

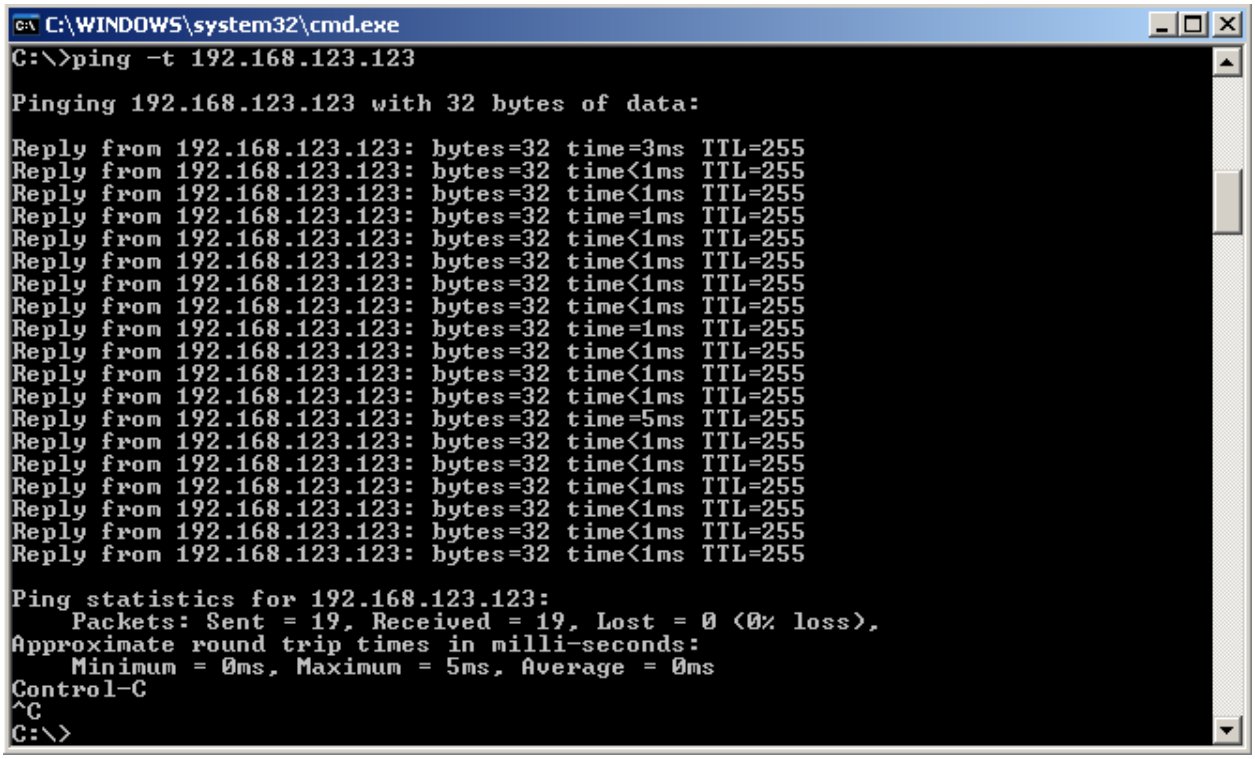
Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating. If, for example, a user can't ping a host, then the user will be unable to send files to that host. Ping operates by sending a packet to a designated address and waiting for a response. The basic operation of Ping can be performed by following these steps in any Windows operating system.

Click on the Start Menu and select Run. Type in “cmd” and enter, you should then see the command screen come up. There will be a certain directory specified (unique to your own PC) with a flashing cursor at the end. At the cursor type the word “ping” leaving a space and the default IP address for the XYR 400E at first startup.

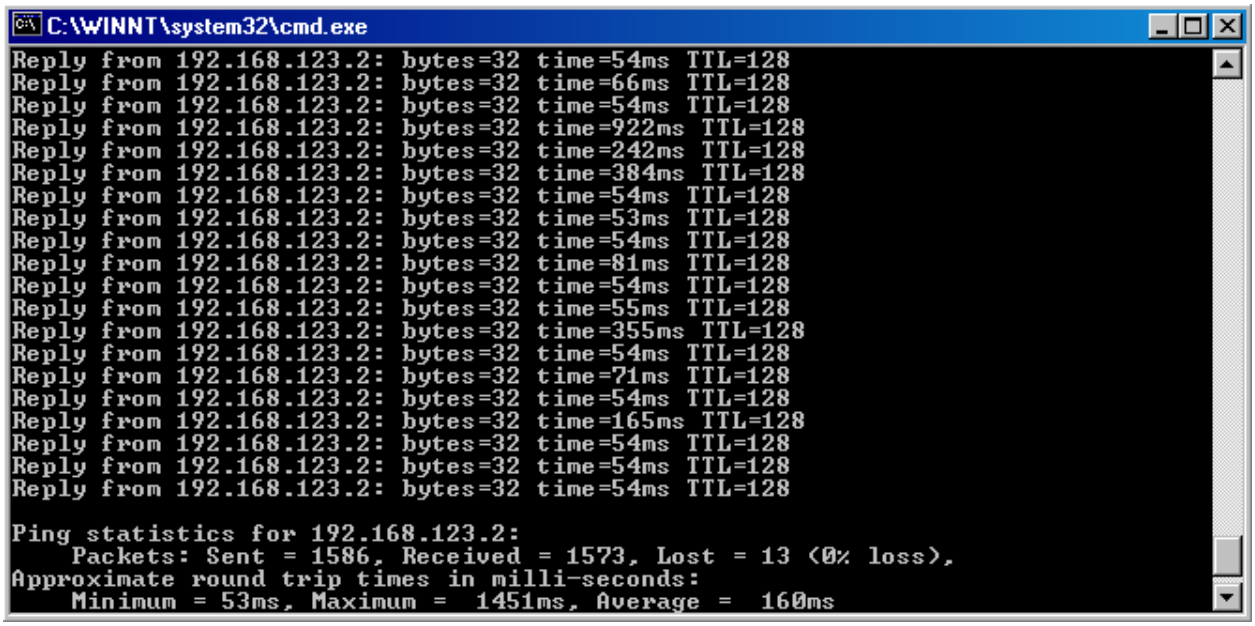
This command would be written as Ping 192.168.123.123 then Enter to send the ping command. The PC will reply with an acknowledgement of your command and if your XYR 400E is correctly configured your reply will look something like this.



The screen shot below shows the response of the “ping 192.168.123.123 –t” command.

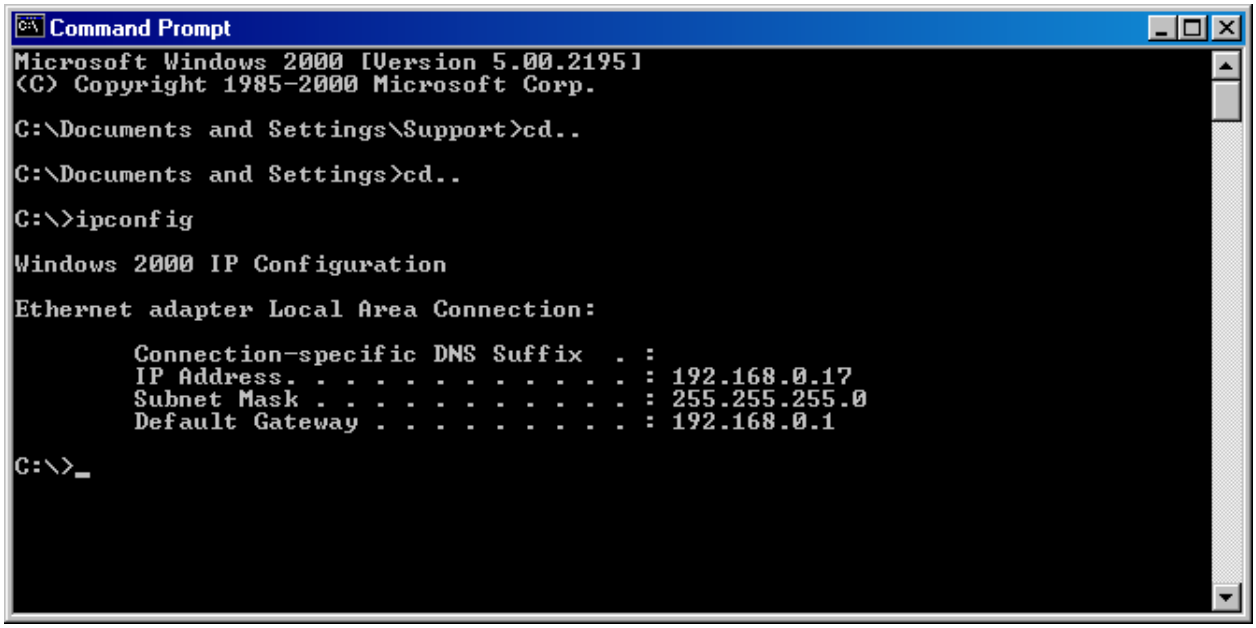

C:\WINDOWS\system32\cmd.exe
C:\>ping -t 192.168.123.123
Pinging 192.168.123.123 with 32 bytes of data:
Reply from 192.168.123.123: bytes=32 time=3ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time=1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time=1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time=5ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Reply from 192.168.123.123: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.123.123:
Packets: Sent = 19, Received = 19, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 0ms
Control-C
^C
C:\>

This -t command is used to repeatedly ping the specified node in the network, to cancel use “Ctrl – C” A good test for the network once it is first set up is to use PING repeatedly from one PC’s IP address to the other PC’s IP address. This gives a good example of the networks reliability and how responsive it is from point to point. When you enter “Ctrl C” the program reports a packet sent-received-lost percentage.


C:\WINNT\system32\cmd.exe
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=66ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=922ms TTL=128
Reply from 192.168.123.2: bytes=32 time=242ms TTL=128
Reply from 192.168.123.2: bytes=32 time=384ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=53ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=81ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=55ms TTL=128
Reply from 192.168.123.2: bytes=32 time=355ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=71ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=165ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Reply from 192.168.123.2: bytes=32 time=54ms TTL=128
Ping statistics for 192.168.123.2:
Packets: Sent = 1586, Received = 1573, Lost = 13 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 53ms, Maximum = 1451ms, Average = 160ms

4.4.2 IPCONFIG

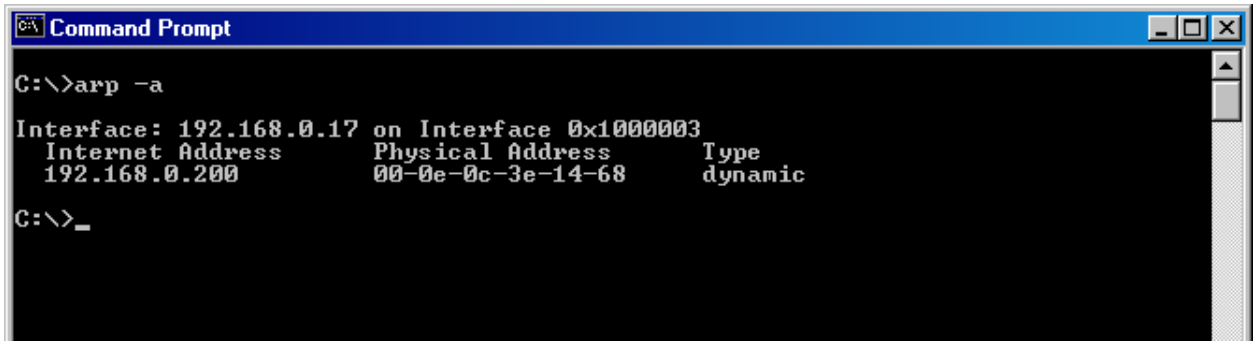
IPCONFIG can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.


Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\Documents and Settings\Support>cd..
C:\Documents and Settings>cd..
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.0.17
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
C:\>

In the above example ipconfig was entered in the command prompt. The reply back shows the PC's IP address, Subnet mask and the gateway it is connected to.
Other ipconfig commands will return back more information. The hardware or MAC address of the computer may be discovered using the command ipconfig /all.
Ipconfig /? will list all of the commands and their usages available for use.

4.4.3 ARP

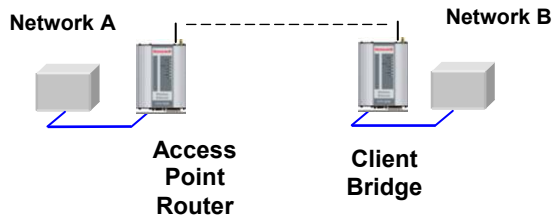
Displays and modifies the IP-to-Physical address translation tables used by Address Resolution Protocol (ARP).
Once a remote computer has been pinged, this can be used to see the IP address & MAC address of the remote computer. It will also show any other devices on the network that it may be connected to.



Command used for above screen shot is Arp –a. It shows the PC's direct IP address of 192.168.0.17 as also shown before with IPCONFIG command. The other IP address shown with its associated MAC address is another device with a connection to the PC. In this example it is the IP address of a PLC connected to the PC also.
Arp –n lists all the commands available for this function.

4.4.4 ROUTE

Route is used for the Router function. This is where you are joining 2 different networks together via the XYR 400E *refer to Section 1.1*
The XYR 400E can only accept 1 Routing table. That is it can only accept one router per network of radios. On the Router radio network PC a routing rule needs to entered to allow access between Network A and Network B. This is entered in the command prompt as per all other instruction above.



Route PRINT will show all active routes on PC,

Route ADD will add a routing table to network,

route DELETE <*destination netmask gateway interface*> will delete the unwanted routing table

route CHANGE modifies an existing route.

An example of a routing table is shown for the configuration below,

Network A Settings
IP Address 192.168.0.17
Subnet Mask 255.255.255.0
Gateway IP 192.168.0.1

Client Bridge Settings
Gateway IP 192.168.2.51
Ethernet IP 192.168.2.50
Subnet Mask 255.255.255.0
Wireless IP 192.168.2.50
Subnet Mask 255.255.255.0

Access Point Router Settings
Gateway IP 192.168.0.1
Ethernet IP 192.168.0.191
Subnet Mask 255.255.255.0
Wireless IP 192.168.2.051
Subnet Mask 255.255.255.0

Network B Settings
IP Address 192.168.2.201
Subnet Mask 255.255.255.0
Gateway IP 192.168.2.51

In the Network A PC a routing rule is to be set.

This will allow Network A & B to have access to each other. This is entered under cmd prompt.

Route ADD 192.168.2.0 MASK 255.255.255.0 192.168.0.191

This says access everything on network B (192.168.2.0) with the Mask of 255.255.255.0 on Network A via the Ethernet IP Interface 192.168.0.191

IP Address 192.168.2.0 will allow everything on this network to be shared by the router. When adding a routing table you will need to enter this in. Once entered in the Router will determine whether to pass information over the router if it is addressed to do so or not. For added security MAC address filtering could be added as mentioned earlier in Section 3.

Chapter Five SPECIFICATIONS

General		
EMC specification	EN 300 683	FCC Part 90
Radio specification	EN 300 328	FCC Part 15.247, RSS 210
Housing	114 x 140 x 30mm 4.5 x 5.5 x 1.2 inch	Powder-coated, extruded aluminum DIN rail mount
Terminal blocks	Removable	Suitable for 12 gauge (2.5sqmm) conductors
LED indication	Active, Serial RX and TX, Radio RX and TX, Link	
Operating Temperature	-35 to +60 degrees C -30 to +140 degrees F	0 – 99% RH non-condensing
Power Supply		
Nominal supply	9 to 30VDC	Overvoltage and reverse voltage protected
Average current drain	240 mA @ 12V	150mA @ 24VDC
Current drain when transmitting	440 mA @ 12V	280mA @ 24VDC
Ethernet Port	10/100 BaseT	RJ45
Standard	IEEE 802.3 compliant	Bridge/router, Access point/ client functionality
Radio Transceiver		
Transmit power	Different models available.	100mW (20dBm) or 300mW (25dBm)
Channels	11 x 5MHz	First channel centre at 2.412 GHz
Receiver sensitivity	< 8% FER	-96dBm @ 1Mb/s, -91dBm @ 11Mb/s
Antenna Connector	Female SMA coaxial	Two connectors for signal diversity
Wireless data rate - configurable	1 to 11Mb/s	“Auto” function determines fastest rate within user-configured fade-margin

Serial Ports		
RS232 Port	DB9 female DCE	RTS/CTS/DTR/DCD hardware signals provided
RS485 Port	2 pin terminal block	Max distance 4000' / 1.2 km
Data rate (bit/sec) - configurable	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200	7 or 8 data bits, Stop/start/parity bits configurable
System Parameters		
System address	1 to 31 character text string	
Wireless data encryption	None, WEP (64bit and 128bit), WPA-PSK (TKIP)	
User Configuration	Via embedded web page	Via RS232 commands, or RS-232 PPP connection
Diagnostics	LED's	OK, DCD, Radio and Serial RX/TX
	RSSI measurement in dBm	BER test

Appendix A FIRMWARE UPGRADE

Determine which firmware version is present in the module to be upgraded by viewing the index webpage of the module.

Firmware versions v1.21 and later may be upgraded via the configuration web pages. This upgrade can be done locally with a PC connected directly to the module, or remotely over a working radio link. For remote upgrade, it is advisable to reduce radio traffic over the link from other devices, as much as possible. If necessary, create a temporary separate radio network to perform the upgrade to remote modules. Please refer to the "Web based Upgrade" section for the upgrade procedure.

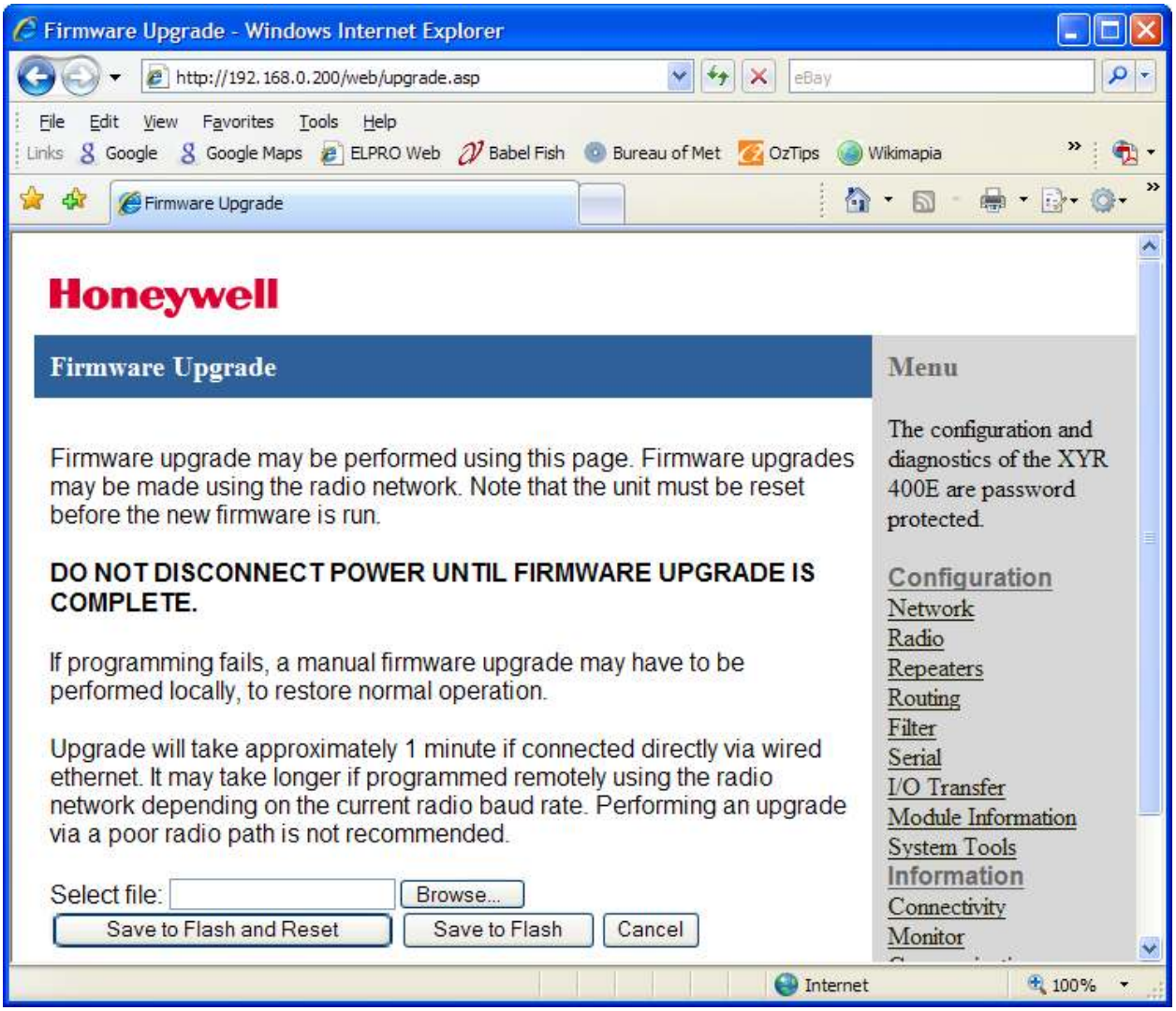
Firmware versions prior to v1.21 require must be upgraded using the *FlashUpdate* utility, and can only be performed local to the module. The FlashUpdate utility should also be used if firmware versions of modules to be upgraded are unknown. The section "Manual Upgrade using Flash Update" outlines the upgrade procedure.

Web based Upgrade

If the module has application firmware version v1.21 or later currently installed, please follow these steps to upgrade the unit.

1. Place the new application firmware file epm_E24G_*x.x*.bin.gz on the computers hard drive. Ensure that the file is not placed in a deeply nested folder.
2. Open internal webpage of unit to be upgraded, and Select System Tools from Menu
3. Select Firmware upgrade from the System Tools menu.

4. Click Browse button and find the application firmware file on your computer. Ensure that the file is not in a deeply nested folder, as there is a character limitation of the filename and path.

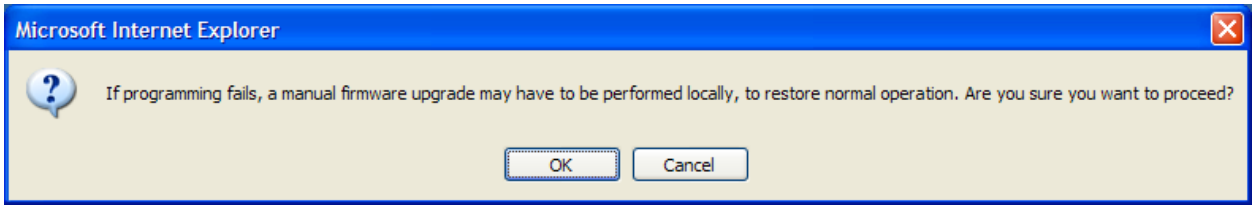

Firmware Upgrade - Windows Internet Explorer
http://192.168.0.200/web/upgrade.asp
File Edit View Favorites Tools Help
Links Google Google Maps ELPRO Web Babel Fish Bureau of Met OzTips Wikimapia
Firmware Upgrade
Honeywell
Firmware Upgrade
Firmware upgrade may be performed using this page. Firmware upgrades may be made using the radio network. Note that the unit must be reset before the new firmware is run.
DO NOT DISCONNECT POWER UNTIL FIRMWARE UPGRADE IS COMPLETE.
If programming fails, a manual firmware upgrade may have to be performed locally, to restore normal operation.
Upgrade will take approximately 1 minute if connected directly via wired ethernet. It may take longer if programmed remotely using the radio network depending on the current radio baud rate. Performing an upgrade via a poor radio path is not recommended.
Select file:
Browse...
Save to Flash and Reset
Save to Flash
Cancel
Menu
The configuration and diagnostics of the XYR 400E are password protected.
Configuration
Network
Radio
Repeaters
Routing
Filter
Serial
I/O Transfer
Module Information
System Tools
Information
Connectivity
Monitor
Internet
100%

5. There are two options:

    a. The “Save to Flash and Reset” button may be clicked, to initiate a reset immediately after a successful firmware upgrade so that the new firmware is run.

    b. Alternatively, Click “Save to Flash” button to just program the new firmware to the unit. A reset is necessary to run the new firmware. This is useful for maintaining radio link whilst performing upgrades to remote units.

6. The following dialog box may be displayed as a warning. Click OK to proceed.


Microsoft Internet Explorer
If programming fails, a manual firmware upgrade may have to be performed locally, to restore normal operation. Are you sure you want to proceed?
OK
Cancel

7. Firmware upgrade will proceed, and should take about 1 minute if performed locally. If performed over a radio link, the upgrade may take longer, depending upon the quality of the radio link, and the amount of traffic on the network.

   During the upgrade, the webpage shows a progress bar at the bottom right side of the browser window.

   When upgrade is completed, the System Tools webpage will be shown if "Save to Flash" was clicked. If "Save to Flash and Reset" was clicked, the unit will display a message that the module is resetting.

   Firmware upgrade is now complete.

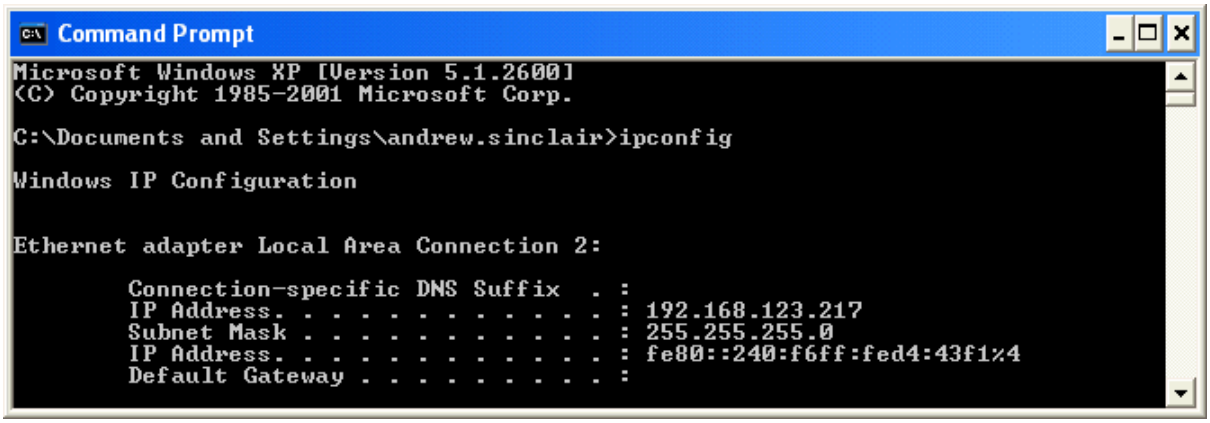
Manual Upgrade using Flash Update

1. Connect the module's ethernet port to PC ethernet port via a "straight through" ethernet cable. "Straight through" ethernet cable is typically a blue colour.

   Alternatively, connect the module to PC via a network switch or hub, as some configurations of Windows can encounter difficulty upgrading without a hub connected. On some PCs, Windows can take much longer than expected to initialise its network interface when the device is reset - connecting via a hub/switch removes this issue during the upgrade procedure.

2. Switch dip-switch on module to **SETUP** mode.
3. **Power up** the module and wait a couple seconds. This will ensure that Windows networking can correctly detect an operating ethernet port.

4. Ensure your PC network settings have a Subnet Mask of 255.255.255.0. This can be easily checked using DOS command IPCONFIG.

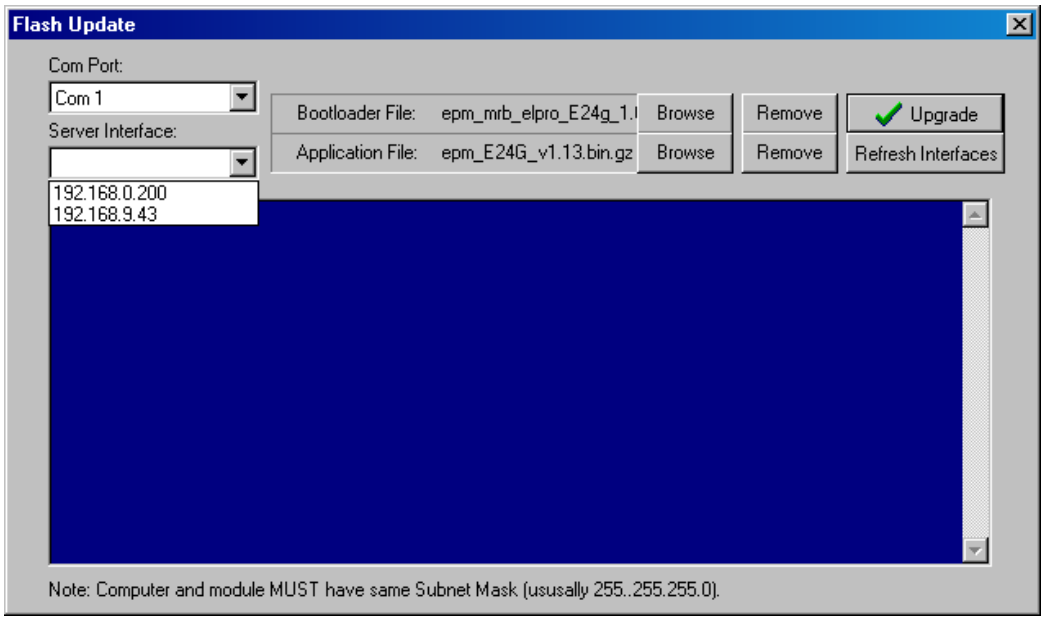

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\andrew.sinclair>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.123.217
Subnet Mask . . . . . : 255.255.255.0
IP Address. . . . . : fe80::240:f6ff:fed4:43f1%4
Default Gateway . . . . . :

5. Extract FlashUpdate program, and start the program.
6. If you are running Windows firewall you may be prompted with the following message. Select Unblock so that FlashUpdate program may operate. If any other firewall software is operating, disable it.

Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: FlashUpdate_1.0
Publisher: Unknown
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

7. Copy new firmware files to a known location on the hard drive of your PC. Do not unzip these files.
8. Specify location of firmware bootloader file (epm_mrb_Honeywell_E24G_*x.x*.bin.gz) and firmware application file (epm_E24G_*x.x*.bin.gz) using the Browse buttons in the FlashUpdate program.
9. Connect PC to module RS-232 serial port with “straight-though” serial cable.
10. Select COM port connected to module in the *FlashUpdate* program.

11. Select Server Interface in the *FlashUpdate program. (IP address of PC connected to which can be found from step 4 above)*

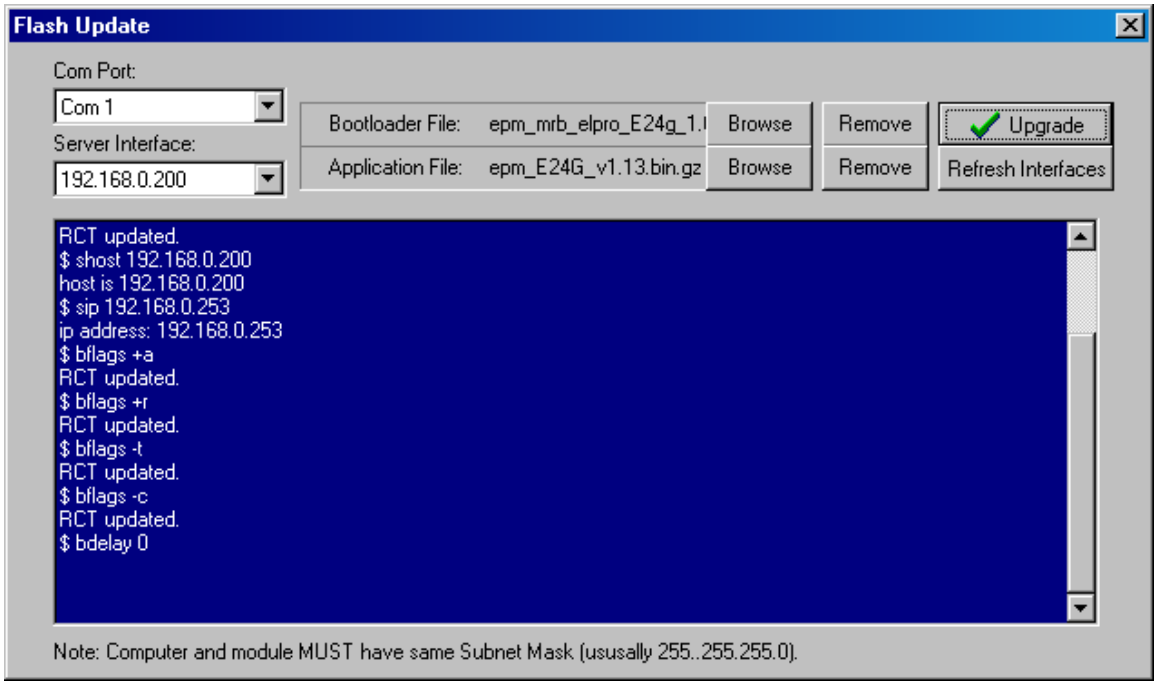


12. Click on *Upgrade* button in *FlashUpdate* program.
13. Follow instructions from confirmation window.

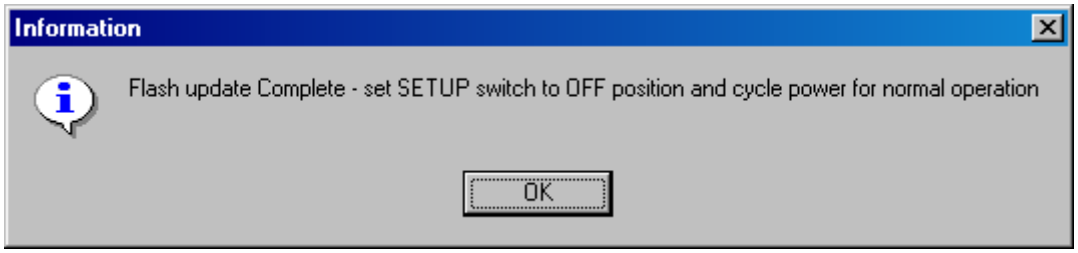
Confirm
Ensure SETUP switch is ON, and RS232 and Ethernet cables are connected to module.
Cycle power to module within 30 seconds after selecting "OK" to this message.
OK

14. Click *OK,* **Power down** module, wait approximately 1 second, and power up module. This entire step must be accomplished within 30 seconds of completing the previous step.

15. Programming will commence…



16. If programming was successful, a dialog box is displayed showing this.



17. Switch dipswitch to RUN position and cycle power for normal operation.

Appendix B GLOSSARY

ACK	Acknowledgment.
Access point	An access point is the connection that ties wireless communication devices into a network. Also known as a base station, the access point is usually connected to a wired network.
Antenna Gain	Antennae don't increase the transmission power, but focus the signal more. So instead of transmitting in every direction (including the sky and ground) antenna focus the signal usually either more horizontally or in one particular direction. This gain is measured in decibels
Bandwidth	The amount of "transportation" space an Internet user has at any given time.
Bridge	Bridges are similar to repeaters or network hubs, devices that connect network segments at the physical layer. Connects multiple network segments at the data link layer.
Collision avoidance	A network node characteristic for proactively detecting that it can transmit a signal without risking a collision.
Crossover cable	A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. Instead of the signals transferring in parallel paths from one set of plugs to another, the signals "crossover." If an eight-wire cable was being used, for instance, the signal would start on pin one at one end of the cable and end up on pin eight at the other end. They "cross-over" from one side to the other.
CSMA/CA	CSMA/CA is a "listen before talk" method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously. Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.
CSMA/CD	A method of managing traffic and reducing noise on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect

	a collision and retransmit after a random time delay.
DHCP	A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.
Dial-up	A communication connection via the standard telephone network, or Plain Old Telephone Service (POTS).
DNS	A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.
DSL	Various technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper POTS (Plain Old Telephone Service) telephone wires.
Encryption key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.
Firewall	Keeps unauthorized users out of a private network. Everything entering or leaving a system's internal network passes through the firewall and must meet the system's security standards in order to be transmitted. Often used to keep unauthorized people from using systems connected to the Internet.
Hub	A multiport device used to connect PCs to a network via Ethernet cabling or via WiFi. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more.
Hz	The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b LANs operate at 2.4 GHz.
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.
Infrastructure	A client setting providing connectivity to an AP. As compared to Ad-Hoc mode,

mode	whereby PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad-Hoc and AP.
I/O	The term used to describe any operation, program or device that transfers data to or from a computer.
Internet appliance	A computer that is intended primarily for Internet access, is simple to set up and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, e-mail services, entertainment and personal information management applications.
IP	A set of rules used to send and receive messages at the Internet address level.
IP (Internet Protocol) telephony	Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).
IP address	A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.
IPX-SPX	IPX, short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services. Sequenced Packet Exchange, SPX, a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.
ISA	A type of internal computer bus that allows the addition of card-based components like modems and network adapters. ISA has been replaced by PCI and is not very common anymore.
ISDN	A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data or video.

ISO Network Model	A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are: Physical , Data Link, Network, Transport, Session, Presentation, Application.
LAN	A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives.
Receive Sensitivity	The minimum signal strength required to pick up a signal. Higher bandwidth connections have less receive sensitivity than lower bandwidth connections.
Router	A device that forwards data from one WLAN or wired local area network to another.
SNR	Signal to Noise Ratio. The number of decibels difference between the signal strength and background noise.
Transmit Power	The power usually expressed in mW or db that the wireless device transmits at.
MAC Address	A MAC address, short for Media Access Control address, is a unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware -- such as wireless cards -- is a security feature employed by closed wireless networks. But an experienced hacker -- armed with the proper tools -- can still figure out an authorized MAC address, masquerade as a legitimate address and access a closed network. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
NAT	Network Address Translation: A network capability that enables a houseful of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
NIC	A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

Proxy server	Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.
RJ-45	Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.
Server	A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.
Site survey	The process whereby a wireless network installer inspects a location prior to putting in a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.
SSL	Commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session
Subnetwork or Subnet	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.
Switch	A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.
TCP	A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

TCP/IP	The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.
VoIP	Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).
VPN	A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.
WAN	A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).
WEP	Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.
Wi-Fi	Wireless Fidelity: An interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.